*Welcome to RELTCO, Inc. Policies & Procedures for Title & Settlement Agents. Intended for compliance with the ALTA's Best Practices v 2.5 effective 10/7/2016.*

***Contact*** us at 1(813)855-0009 or email at ReltcoCompliance@Reltco.com

**Satellite Offices:**

**TEXAS OFFICE**
101 East Park Blvd Ste 600
Plano, TX 75074

**ALABAMA OFFICE**
3829 Lorna Road Ste 322
Birmingham, AL 35244

**NEVADA OFFICE**
871 Coronado Center Drive Ste 200
Henderson, NV 89052

**RELTCO OF UTAH**
960 S Main Street Ste 2B
Brigham, UT 84302

**RELTCO OF ARKANSAS**
17724 Interstate 30 Ste 2 Unit 8
Benton, AR 72019

**Company Name: RELTCO, Inc.**

**Date all policies will go into effect: 12/1/2016**

RELTCO INC.
RESIDENTIAL AND COMMERCIAL TITLE COMPANY

# RELTCO, Inc.

# LICENSING AND BUSINESS REGISTRATION POLICY

**Effective 12/1/2016**
**Revised Date:**

**Best Practices Policy #1- Licensing:** RELTCO, Inc. will establish and maintain current License(s) as required to conduct the business of title insurance and settlement services. We will maintain appropriate and necessary licenses for all employees providing title insurance services for which a license is required and will maintain our business in good standing with the state. We will also maintain all required licenses to use third party products and services, including software and ALTA forms licenses.

Procedures we will follow to meet this Policy are:

- Obtain and maintain all required state and/or local business registrations and License(s).
- Obtain and maintain compliance with licensing, registration, or similar requirements with the applicable state regulatory department or agency for the Company and all individuals who are required by state law to be licensed or registered.
- Maintain compliance with ALTA's Policy Forms Licensing requirement.

A listing of our current licenses is attached. This list will be updated on not less than an annual basis.

## Licensing Checklist

| Individual/Company Name* | State | License number | License Type | Expires |
|---|---|---|---|---|
| | | | | |
| SEE RELTCO BEST PRACTICES FILE FOLDER POLICY 1 | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

***Attach copies of all licenses, including insurance licenses, business licenses (Department of State registration), ALTA Membership or forms license, law license, etc. for quick reference.**

# RELTCO, Inc.

# TRUST ACCOUNTING POLICIES AND PROCEDURES

**Effective Date: 12/1/2016**

**Revised Date:**2/15/17

**Best Practices Policy #2- Trust Accounting:** We have adopted and maintained appropriate written procedures and controls for Escrow Trust Accounts allowing for electronic verification of reconciliation. Appropriate and effective escrow controls and staff training help title and settlement companies meet client and legal requirements for the safeguarding of client funds. These procedures help ensure accuracy and minimize the exposure to loss of client funds. The protection of our clients' funds is an integral part of what we do and is mandatory both to protect our clients and our company from financial harm. Compliance with the following procedures is required of all employees and failure to comply with the procedures outlined herein will be grounds for immediate termination of employment.

**A. Separation of Funds:**

To prevent the accidental or intentional mixing of escrow funds with other funds, we will:

1. Ensure all bank accounts containing fiduciary funds are styled as "Escrow" or "Trust". The words "Escrow Account" or "Trust Account" will be included on the signed bank agreement, on the bank statement, disbursement checks and deposit slips. Such accounts are only to be utilized for escrow or trust transactions. Operating funds are never to be comingled with escrow funds.

2. Maintain all escrow funds, including sweep accounts, in Federally Insured Financial Institutions.

3. Hold underwriter premiums in trust (commonly known as 'Compliance Account') and do not comingle with the agency's operating accounts.

**B. Identification of the nature, Amount and Reason Funds are Held**

To ensure that we can adequately identify the ownership of funds we hold in trust, we will:

1. Assign a unique sequential number or unique identifier to each closing file, auto assigned by software system Resware.

2. Maintain written documentation of the reason for escrow file balances being held longer than six months. Require management approval for disbursements from these files.

3. Include file numbers on all escrow checks and deposit slips to provide a clear and direct connection between the documents and the related file.

4. Prepare a separate deposit slip for each file to provide a direct connection between the amount of the deposit as shown on the bank statement and the amount as shown on the file's ledger. Electronic software system receipt.

**C. Reconciliations:**

On a daily basis we will, at a minimum, have the reconciler access our fiduciary bank account activity online and clear all receipts and disbursements for each fiduciary account. Any discrepancies will be investigated immediately. Items that are not resolved will be reported to management.

On not less than a monthly basis, we will:

1. Prepare a monthly escrow trial balance for each escrow account (and any other fiduciary account) which, at a minimum, lists all open escrow balances.

2. Complete a monthly three way reconciliation within ten (10) days of the closing date of the bank statement for each escrow account. This will include a reconciliation of bank balance, book balance, and escrow trial balance for each escrow bank account (and any other fiduciary account).

3. Have someone who is not a signatory on the escrow accounts and who is unassociated with the receipt or disbursement functions perform the three way reconciliation. **(Terry Duvall)**

4. Include copies of all checks, wire documentation, deposit slips, and receipt items with the escrow reconciliations. If a bank does not return actual canceled checks with bank statements, we will ensure that copies of all checks are maintained in our records or we will obtain a signed acknowledgement that our bank will provide copies upon request. Check copies, from any source, will meet the following criteria:

   (a) The copies of all checks will be clearly legible;

   (b) The copy will include both sides of every check so that endorsements can be verified; and

   (c) It will be unmistakable which front and back images belong together.

5. Include the following procedures in the three-way reconciliation:

   (a) Immediately research and resolve any stale dated outstanding deposits as listed on the outstanding deposit report.

   (b) Immediately research and resolve any unusual outstanding checks, such as:

      (i) Checks payable for recordings outstanding for more than thirty (30) days;

      (ii) Payoffs outstanding for more than ten (10) days;

      (iii) Taxes and hazard insurance payments outstanding for more than thirty (30) days;

      (iv) Underwriter premium outstanding for more than sixty (60) days; and

      (v) Other checks outstanding for more than ninety (90) days.

   (c) Immediately research and resolve any shortages or unusual balances on the trial balance.

   (d) Immediately upon discovery, we will reimburse all escrow receivables and other escrow shortages from our operating account funds.

   (e) Research adjustments that were required to bring the account in balance. We will then post corrections to the proper file so the adjustment can be cleared on the next reconciliation.

   (f) Designated to: Anthony Pautauros, back up Christopher Howell, as Director of Operations will approve each three-way reconciliation and initial and date to indicate review.

   [*Alternative if this is not possible or practical due to agency size]* At a minimum, each reconciliation will be reviewed by another management designated employee, and initialed and dated to indicate the review.

(g) Copies of the completed reconciliations will be scanned and maintained in the “Escrow Reconciliation” folder on the company server.

**Designated duty to: Terry Duvall, Accounting/Reconciliations**

**D. Actions Requiring Management Approval:**

The following may not be performed by any employee absent management's written authorization:

1. No outstanding check may be voided and reissued without Management approval;

2. No funds may be transferred between closing files or escrow accounts absent Management approval. When funds are transferred between accounts or files, the reason for the transfer shall be documented. Documentation of the reason for transfers between closing files shall be maintained in both files.

**E. Interest-bearing (investment) escrow accounts:**

(a) The investment account must be styled in the name of the owner/beneficiary of the escrow funds, with the escrow agent named as trustee or escrow agent.

(b) We must receive written instructions from the owner/beneficiary of the escrow funds to open an investment account. Such written instructions must be maintained in the closing file.

(c) The tax Identification number used to open the interest-bearing escrow account must be that of the owner/beneficiary of the funds.

(d) The interest-bearing escrow account must be included on a control ledger or trial balance that identifies all interest-bearing accounts. The interest must be posted to the escrow account timely following receipt of the statement or other documentation reporting the interest accrued.

**F. Internal Controls:**

To further safeguard our client's funds, we have instituted the following internal control procedures. We will:

1. Verify receipts posted to the validated deposits daily.

2. Utilize positive pay if available in the local marketplace, and have policies & procedures in place that prohibit or control the use of ACH transactions and international wire transaction to protect against unauthorized transactions.

3. Perform a criminal and public records background check going back at least five (5) years is performed when a new employee is hired and is performed on all employees with escrow signatory authority and/or wire initiation and confirmation authority at least every three years thereafter. The checks for Criminal Offenses will include Dishonesty Offenses (involving dishonesty, a breach of trust, or money laundering) and Violence Offenses (felony or its equivalent, or multiple misdemeanors or their equivalents).

*4.* Conduct ongoing training for employees in proper management of escrow funds and escrow accounting.

5. Not less than annually, agency management will review authorized signers and authority limits to ensure they are still at appropriate levels.

**6.** Ensure that all terminated employees are immediately removed from the accounts, and new signature cards executed.

7. We safeguard unused check inventory by keeping it in a secure location and limit access to authorized individuals, only

8. Two signatures are required on all escrow checks, with exception to State of Texas where agency size allows 1 signature per state guidelines.

9. We do not permit the use of signature stamps on escrow checks.

10. We adhere to state escheatment laws.

11. We remove signature blocks from voided checks or otherwise render them ineffective.

12. We discourage the receipt of cash and never accept cash in an amount in any amount.

13. We utilize effective internal controls over wire transfers, including:
    a) proper segregation of authorization, initiation and verification of wires;
    b) review of supporting documentation (e.g., written escrow agreement, closing statements, instructions, etc.) prior to execution of wires out;
    c) immediate verification of bank advices against escrow authorization and instructions;
    d) use of personal identification numbers; and
    e) use of independent call backs.

14. We research inactive/old escrow accounts to ensure all funds are properly disbursed to the appropriate parties and the account can be closed. Funds transferred to active accounts are done on an individual file basis to ensure the funds are kept in their respective files. We always request a final statement showing a zero balance and “closed account” from the bank if one is not sent to the agency.

15. To ensure funds can be reconciled properly, we open a new escrow/trust account anytime we switch to or implement a new closing software system.

| Training & Hiring/Background Checks – Trust Accounting Procedures and Controls | | | | |
|---|---|---|---|---|
| **Employee** | **Title or Role** | **Date employee received the Company's Policy for Trust Account Controls** | **Date employee returned receipt and compliance affidavit** | **Date of Last Background Check** |
| Brian Gaddis | Funding Team Lead | 12/29/2014 | 12/29/2014 | 12/29/2014<br>4/20/2016 |
| ~~Joseph Gucciardo~~ | ~~Funder~~ | ~~04/04/2016~~ | ~~04/04/2016~~ | ~~10/21/2015~~ |
| Milan Takacs | Funder | 5/16/2016 | 5/16/2016 | 05/17/2016 |
| Marlene Cecala | Funder | 05/24/2016 | 5/24/2016 | 5/25/20/16 |
| Terry Duvall | Accounting/Reconciliations | 10/17/2016 | 10/17/2016 | 10/19/2016 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Updated:__10/19/2016**

**2/15/17_____**

**RELTCO, Inc.**
**BANK ACCOUNT LISTING**

*List **all** active and inactive fiduciary accounts (IOLTA, escrow, trust, premium, recording, interest bearing escrow trust accounts, etc)*

| Bank Name | Account # (last 4 digits) | Type (Escrow, IOLTA, etc) | Active or Inactive | Signatories |
|---|---|---|---|---|
| See Best Practices Policy 2 Trust Accounting Bank Account Listing | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

*I hereby certify this is a complete listing of all active and inactive fiduciary accounts (escrow, trust, premium, recording, interest bearing escrow trust accounts, etc.).*

Name

Title Date

**AFFIDAVIT OF RECEIPT AND COMPLIANCE (to be signed by all employees with access to the Escrow Account)**

I acknowledge receipt of the following:

- Policy for Trust Accounting

and agree, as a condition of continued employment by RELTCO, Inc. to abide by and comply with the policies, procedures and requirements as set forth therein.

**See Best Practices Policy 2 Trust Accounting Trust / Escrow Account acknowledgement**

# RELTCO, Inc.

# PRIVACY AND INFORMATION SECURITY POLICIES AND PROCEDURES

**Effective Date 12/1/2016**

**Revised Date:**

**Best Practices Policy #3- Privacy and Information Security:** RELTCO, Inc. has adopted the following policies and procedures to document our information security program to protect Non-public Personal Information as required by local, state and federal law (including the Gramm-Leach-Bliley Act) require. The program is appropriate to the size and complexity of our company and the nature and scope of our activities. Compliance with the following procedures is required of all employees and failure to comply with the procedures outlined herein will be grounds for immediate termination of employment.

Our company recognizes we must take necessary and appropriate steps, within our capabilities, to protect Non-public, Personal Information (NPI) from loss or misuse to avoid reputational damage and to prevent the use of this data from adversely impacting our customers and business. The protection of this data is a critical business requirement, yet flexibility to access the data and to work efficiently with it was also considered in the development of this policy. This policy will be evaluated annually, and adjusted in the event our business operations change or in light of relevant circumstances.

For the purposes of this policy Non-public Personal Information (NPI) is defined as "First name or first initial and last name coupled with any of the following: Social Security Number, Driver's license number, state issued ID number, credit card number, debit card number or other financial account numbers." "Personal Information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

**A. Physical security of Non-public Personal Information (NPI)**

To help ensure the physical security of all Non-public Personal Information we will:

1. Restrict access to Non-public Personal Information to authorized employees with a legitimate business purpose, on a need to know basis.

2. Perform a criminal and public records background check going back at least five (5) years is performed when a new employee is hired and is performed on all employees that will have access to NPI. These checks for Criminal Offenses will include Dishonesty Offenses (involving dishonesty, a breach of trust, or money laundering) and Violence Offenses (felony or its equivalent, or multiple misdemeanors or their equivalents) principally involving violence or harassment for any employee with customer contact. A background check will be performed at least every three years thereafter.

3. Restrict the use of removable media unless authorized by management and properly secured and stored when not in use.

4. Use only secure methods of transmitting NPI

5. Adhere to a "clean desk" policy during the work day where all files (hard copy or electronic) are closed and locked when employees are away from their desk, and stored in locked desk, file cabinet, or secure room overnight.

6. Share information with third parties and affiliated or related parties only in accordance with our Privacy Notice which shall be provided to all parties at closing **and** which will be posted on our website.

**B. Network Security of Non-public Personal Information**

To help ensure the secure collection, transmission, and storage of Non-public Personal Information within our network we will:

1. Take appropriate steps to protect the security of our computing network to include, firewalls, up to date virus protection, and intrusion detection and prevention systems.

2. Utilize strong, individual, and unique passwords that are changed at least every 90 days. A strong password is at least 8 characters in length and contains 3 of the following 4 types of characters (lower case letters, upper case letter and special characters)

3. Encrypt any email transmission containing NPI, or encrypt the gateway between communicators.

4. Provide our employees with our "*Acceptable Use of Information Technology Policy*" (see attached) that is acknowledged annually. This helps assist our staff and other authorized users in conducting the tasks associated with their job and remain in compliance with the Privacy Policy of RELTCO, Inc. (see attached) and all relevant federal and state laws and regulations protecting NPI.

**C. Disposal and Maintenance of Non-public Personal Information**

To help protect and properly dispose of Non-public Personal Information we have:

1. Clearly defined and communicated to our employees what types of information/data fall into the category of NPI. A definition of NPI is provided in the beginning of this policy.

2. We securely maintain and dispose of records and equipment containing NPI pursuant to the timeframes established on the Risk Assessment, attached

3. Provided shredders or locked disposal bins accessible only by an outside shredding service.

4. Required all hardware containing NPI that is to be disposed of to be erased/encrypted or physically destroyed prior to disposal.

**D. Establish a Disaster Management Plan**

The company has established a *Disaster Management Plan* (attached). This plan helps ensure adequate back-up, recovery and business continuity procedures for our company. This plan is reviewed and updated annually or as appropriate.

**E. Appropriate Management and Training of Employees to Help Ensure Compliance with the Information Security Program of RELTCO, Inc. .**

To ensure appropriate management of our policy, and employee training regarding the Company's information security policy we:

1. Provide all employees with a copy of our Acceptable Use of Information Technology Resources policy and obtain signed acknowledgements of receipt.(attached)

2. Review our Information and Data Privacy Policy annually to detect the potential for improper disclosure of confidential information and update as appropriate.

3. Oversee all third party service providers, including third party signing providers, to help ensure compliance with our Company's information security program. We retain service providers that are capable of appropriately safeguarding NPI and have either agreed to do so in our contract or have otherwise demonstrated that they protect NPI in accordance with our policy. If security breaches occur, proper notification is provided to consumers and law enforcement in accordance with the Company's privacy and information security program.

**F. Notification of Security Breaches to Customers and Law Enforcement**

To ensure proper notification of security breaches to our customers and law enforcement we will:

1 Post our Information and Data Privacy Policy on our website (or provided to our customers at closing if no website exists).

2 Adhere to our procedure to notify our customers and law enforcement of the breach as required by law or contract. All data breaches will be reported and investigated in a timely manner. In the event of a breach, employees will immediately notify a supervisor or agency management. The data will be secured to prevent any further breach, and the reasonable integrity, security and confidentiality of the data or data system will be restored.

3 Contact our IT department (or IT contractor) to help determine the nature of the breach in terms of its extent and seriousness. We may also contact our Legal Department (or Attorney) to help determine the category of the breach.

4 Document the breach, the scope of the breach, steps taken to contain the breach, and the names or categories of persons whose personal information was, or may have been, accessed or acquired by an unauthorized person.

5 Provide the documentation on the breach to senior management who will direct that notification be given to affected parties if the breach appears to have resulted in the theft or loss of NPI.

6 Provide notification of a breach to affected individuals without unreasonable delay except that notification shall be delayed if law enforcement informs the Company that disclosure of the breach would impede a criminal or other investigation. A request for delayed notification must be made in writing including the name of the law enforcement officer making the request and the officer's agency engaged in the investigation. Such delayed notification shall continue until the law enforcement agency communicates to RELTCO, Inc. its determination that notification will no longer impede the investigation.

7 Ensure the notification is clear and conspicuous and includes the following:
   a. A description of the incident in general terms;
   b. A description of the type of personal information that was subject to the unauthorized access and acquisition;
   c. A general description of the actions taken to protect the personal information from further unauthorized access.
   d. A telephone number that the person may call for further information and assistance;
   e. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports;
   f. The toll-free numbers and addresses for the major consumer reporting agencies: and the toll free numbers, address, and website address for the Federal Trade Commission (FTC) and the Attorney General's Office for the state in which the victim is located, along with a statement that the individual can obtain information from these sources about preventing identify theft.

8. Notify the affected persons by one of the following methods:

    a. If we can identify the particular individuals affected and have the necessary contact information of the affected individuals, notice will be provided in writing by US Postal Service or by electronic notification if the Company has a valid email address.

    b. If we do not have the necessary contact information to notify an individual or are not able to identify particular affected individuals, notice will be provided by a conspicuous posting on the Company's website and publication in widely distributed print media in the states where affected individuals are reasonably anticipated to reside.

| Training & Hiring/Background Checks<br><br>PRIVACY AND INFORMATION SECURITY<br><br>Procedures and Controls | | | | |
|---|---|---|---|---|
| **Employee** | **Title or Role** | **Date employee received the Company's Procedures for Privacy and Information Security** | **Date employee returned receipt acknowledgement** | **Date of Last Background Check** |
| **All items can be obtained upon request**<br><br>**Personnel files are housed in HR office** | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Updated:_____**

**NPI Security Risk Assessment** (please complete for all areas where NPI may be located. Include all outside vendors who have access to NPI)

| **Location of NPI (for example, files, server, computers, laptops, cell phones, emails containing NPI, thumb drives, CD, etc.)** | **Risk of breach** | **Method for Securing** | **Retention** | **Method for disposal** |
|---|---|---|---|---|
| *Server* | *Low* | *Locked in server room* | *7 years* | *Secure destruction* |
| *Sales Laptop (no NPI access)* | *Low* | *Encrypted and password protected* | *7 years* | *Secure destruction* |
| *Workstation Desktops* | *Low* | *Password protected* | *7 years* | *Secure destruction* |
| *Settlement Files* | *Medium* | *Password protected* | *7 years* | *Secure Destruction, Secure shredding* |
| *After-hours company Cell Phones* | *Low* | *Phones are encrypted and require a 4-digit PIN to access* | *Until phone is taken out of service or employee is terminated* | *Remote Wipe* |
| *Emails containing NPI ZixCorp Secure Encryption Eff 01/01/2017* | *Low* | *Encryption through secure gateway with communicator Adding ZixCorp Secure* | *4 years* | *Backup to server and deleted* |
| *Bank statements and reconciliations* | *Low* | *Locked in file cabinets Password protected desktops, server* | *7 years* | *Secure shredding Secure destruction* |
| | | | | |
| | | | | |
| | | | | |

## RELTCO, Inc.

## Vendors with access to NPI and Third Party Signing Professionals Listing

| Outside Vendors with access to NPI | Risk of breach | Method for ensuring that vendor will protect NPI |
|---|---|---|
| *Legal Shred* | *Low* | *Contract* |
| *Vology IT Services* | *Medium* | *Service Provider Agreement* |
| *Contract Closing/Notary Services* | *Medium* | *Service Provider Agreement* |
| | | |
| *Apex Office Supplies* | *Low* | *Service Provider Agreement* |
| *Fed Ex* | *Low* | *Service Provider Agreement* |
| *UPS* | *Low* | *Service Provider Agreement* |

Note: Third Party Signing Professionals require additional oversight, as provided in our Policies & Procedures over Settlement, Recording & Pricing.

# Service Provider Agreement

The undersigned, as a service provider for RELTCO, Inc. , hereby agrees that in providing services for the company will comply with State and Federal law and regulations regarding the safeguarding of consumer Nonpublic Personal Information (NPI) as well as the company's Privacy Policy, attached hereto, and will implement the following safeguards guidelines in order to protect the security, confidentiality, and integrity of customer information:

- Access to customer information will be limited to the person(s) performing the services requested by RELTCO, Inc. .
- All customer information will be utilized only for purposes of the services being provided.
- Customer information will not be shared or disclosed and will be protected from theft by electronic means or otherwise.
- All areas where customer information will be stored are protected from physical hazards, included but not limited to, floods and fires.
- The undersigned will assure that all of its employees will comply with the terms of this agreement.

For purposes of the Agreement, the following terms have the following meanings:

"Customer Information" means any record containing nonpublic personal information about a customer or financial institution, whether in paper, electronic, or other form that is handles or maintained by or on behalf of the financial institution or its affiliates.

"Nonpublic personal information" (NPI) means any information that a consumer provides or that is obtained in connection with a financial product or service that is not available from public sources, such as land records and government records.

In executing this Agreement, the undersigned agrees to comply with all the terms and conditions set forth herein and set forth in RELTCO, Inc. 's Privacy Policy.

Company Name:_____

Company Address:_____

Authorized Representative Name:_____

Authorized Representative Title:_____

Phone Number:_____

Email:_____

Authorized Representative Signature:_____

Date:_____

**AFFIDAVIT OF RECEIPT AND COMPLIANCE (To be signed by all employees)**

**All items can be obtained upon request**

I acknowledge receipt of the following:

- Privacy and Information Security Policy
- Acceptable Use of Information Technology
- Privacy Policy
- Disaster Management Plan

and agree, as a condition of continued employment by , RELTCO, Inc. to abide by and comply with the policies, procedures and requirements as set forth therein.

**All items can be obtained upon request**

**Personnel files are housed in HR office**

# RELTCO, Inc.

# ACCEPTABLE USE OF

# INFORMATION TECHNOLOGY RESOURCES POLICY

Effective Date 12/1/2016

**Revised Date:**

RELTCO, Inc. ("Company") Information System Resources are essential to Company operations. Users have been given selective access to this hardware, services, software and data for the purpose of completing the tasks required by their position.

RELTCO, Inc. is committed to the responsible use of our Information System Resources in support of its business.

**Policy Principles**

1. RELTCO, Inc. Information System Resources are provided to assist staff and other authorized users in conducting the tasks associated with their position.

2. All users are responsible for using RELTCO, Inc. Information System Resources in an honest, ethical, and legal manner and with regard to the privacy, rights, and sensitivities of other people. Use must be in accordance with the Company's policies and all relevant federal and state laws and regulations. Such laws and regulations include, but are not limited to, laws and regulations pertaining to privacy, copyright, freedom of information, equal employment opportunity, intellectual property and occupational health and safety.

3. RELTCO, Inc. IT personnel should always be contacted if there is any question about the proper use of [Company Name] Information System Resources.

4. The following general principles apply to usage of RELTCO, Inc. Information System Resources:
    a. Each authorized user of RELTCO, Inc. Information System Resources is assigned a user account, which is identified by username.
    b. Only authorized users may use RELTCO, Inc. Information System Resources and may only use those IT resources to which they are authorized.
    c. Where access to resources is protected by a password or other authorization protocol, and a user must not make this available to any other person. Users who do so will be held responsible for all activities originating from that account.
    d. A user must not use an account setup for another user nor make any attempts to find out the password of a resource they are not entitled to use.
    e. The above does not apply where a user provides access to their account to an authorized IT support person.
    f. Users may be given a range of IT resources and must use any and all of these resources in a manner that is ethical, lawful, effective and efficient.
    g. The Company discourages the storing of passwords due to the security risk this poses.

h. Each user, while using their account, is responsible for:

   i. All activities which originate from their account;

   ii. All information sent from, intentionally requested, solicited or viewed from their account;

   iii. A user must:
      1. show restraint in the consumption of resources;
      2. apply business and professional integrity;
      3. respect intellectual property and the ownership of data and software;
      4. respect others' right to privacy and freedom from intimidation, harassment and annoyance; and
      5. abide by the RELTCO, Inc. 's policies regarding privacy;

   iv. No user shall:
      1. attempt to subvert the security of any RELTCO, Inc. Information System Resource;
      2. attempt to create or install any form of malicious software which may affect computing or network equipment, software, or data;
      3. attempt to create or install any form of software or script without prior authorization from the IT department;
      4. attempt to interfere with the operation of RELTCO, Inc. Information System Resources;
      5. attempt to subvert any restriction or accounting control of any Information System Resource; or
      6. attempt unauthorized access to RELTCO, Inc. Information System Resources

   v. RELTCO, Inc. Information System Resources, including email and web servers and other similar resources, may not be used for:
      1. the creation or transmission of any material or data which could reasonably be deemed as offensive, obscene, or indecent;
      2. the creation or transmission of material which the average person deems likely to harass, intimidate, harm, or distress;
      3. the creation or transmission of defamatory material;
      4. the transmission of material that infringes on the copyright of another person;
      5. the unauthorized transmission of material that either is labeled confidential or is not generally available from a public source;
      6. the transmission of any material that contravenes any relevant federal or state laws or regulations; or
      7. the deliberate unauthorized access to Information System Resources.

   vi. No user shall use RELTCO, Inc. Information System Resources for personal gain or for the financial gain of a third party.

**Privacy**

1. RELTCO, Inc. seeks to comply with the expectation of privacy and confidentiality in the provision of all IT services, but privacy and confidentiality cannot be assured. Users must know that the security of data and networks can be breached – most people respect security and privacy protocols but a determined person can breach them. Users must also be aware that network and system administrators, during the performance of their duties, need to observe the content of certain data, on storage and in transit, to ensure proper function on the Company's IT services.

2. In addition, any privacy may be subordinate to application of law, regulations or policy, including this policy.

**Network**

1. Users should have no expectation of privacy of network traffic although the Company will make reasonable attempts to keep traffic private.

2. Users should make every attempt to use secure protocols when accessing the network services especially where sensitive or private information is transmitted. This applies particularity to electronic mail.

3. Users should be aware that many protocols transmit authorization detail (i.e. username and password) in an unsecure manner and any transmission of customer NPI in an unsecured manner is prohibited.

**Data**

1. A user must not examine, disclose, copy, rename, delete, or modify data without the express or implied permission of its owner. This includes data on storage devices and data in transit through a network.

2. A user must respect the privacy and confidentiality of data stored or transmitted on the Company's resources. Any release of data to those not authorized to receive it is expressly forbidden.

3. Users storing or transmitting data of sensitive nature, such as information on individuals whether for operations, administrative, or services use must ensure that the privacy of such information is not compromised, In such cases access controls, such as file or database authentication and encryption, should be employed. File access control can be set with the help of the IT department. Simple encryption can be achieved using windows compression and password.

4. In cases where the computer system being used supports file ownership and file access control, files owned by a user should not be accessible to other users. However, in cases where the system supports access control, it is the user's responsibility to ensure their files have appropriate access control settings to ensure the desired level of privacy and integrity. Wherever possible, systems shall be configured so that the default file permissions on a user file will ensure the owner of the file can access the content.

5. All smart phones or mobile devices with @[Company Email ] email account(s) setup that gather and hold emails for later viewing and off line use must be password protected with a min. of 4 characters. Encryption must also be enabled. All devices must be annually reviewed for proper device settings and a confirmation email sent to the IT department. The Company has the right to remotely wipe the data on the device if lost, stolen, or it is found to be in violation of this policy.

6. The Company has the legitimate right to capture and inspect any data stored or transmitted on the Company's systems (regardless of data ownership) when investigating system problems or potential security violations, to maintain system security and integrity, and to prevent, detect, or minimize unacceptable behavior on the systems. Such data will not be released to persons within or outside of the Company, except:
    a. With permission from the user;
    b. Upon written request from a member of senior management based upon reasonable cause;
    c. Where deemed appropriate by the Company in order to uphold the statutory rights of individuals in matters such as privacy, copyright, occupational health and safety, equal employment opportunity, harassment and discrimination;
    d. Upon a proper request from an authorized law-enforcement officer investigating an allegedly illegal act and based on a properly issued court order; or
    e. In accordance with relevant statutes and regulations.

7. The IT department should be notified immediately if a user suspects that data security or data itself is being breached in any way.

**Equipment**

1. Users must take due care when using IT equipment and take reasonable steps to ensure that no damage is caused to IT equipment.

2. Users must not use the equipment if they have reason to believe it is dangerous to themselves or others to do so.

3. Users must report any damage to IT equipment to the IT department.

4. No user shall, without proper authorization:

    a. Attach any device to the RELTCO, Inc. 's IT resources

    b. Connect any equipment to the RELTCO, Inc. 's IT resources that will extend access or provide off-site access to the Company 's resources without prior written approval of IT and Senior Management, which approval shall be based on a determination that such connection meets the Company's security standards.

    c. Tamper with or move installed IT resources without authorization

5. User owned equipment must not be connected anywhere in the network behind the firewall. User owned devices can be connected outside using a wireless connection. Note that user owned devices connected outside the firewall still are subject to usage considerations and restrictions.

**Non-RELTCO, Inc. use of IT resources**

1. RELTCO, Inc. 's IT resources, including telephones, facsimiles, mobile telephones, desktop and laptop computers, printers, photocopiers, email, Internet, web services and similar resources are acquired, installed and commissioned for the Company's business purposes. Use for incidental personal purposes ( Non-business use) may occur but only if that use does not:
    a. Interfere with the Company's operations or information technology;
    b. Interfere with others' use of IT resources;
    c. Burden the Company with additional costs;
    d. Interfere with the user's employment or other obligations to the Company; or
    e. Constitute an offense under any relevant laws or regulation.

2. Where a supervisor reasonably believes misuse has occurred, and such misuse persists after appropriate warning, restrictions may be applied on the user's access to the Company's IT resources or discipline may be taken under the Company's disciplinary procedures.

**Administration and Implementation Compliance**

1. RELTCO, Inc. treats misuse of IT resources seriously. Violations of the conditions of use of IT resources may result in temporary or indefinite withdrawal of access, disciplinary action and reimbursement to the Company.

2. A user's access will be withdrawn upon written request from an appropriate user, supervisor or resource owner.

3. Misuse or unauthorized use of the Company's IT resources may constitute an offense under federal or state laws and/or regulations. Nothing in this policy or the requirements governing the use of IT resources may be taken as in any way diminishing or removing a person's obligations to comply with the law, or their liability to prosecution and punishment under law.

4. Users are encouraged to report any misuse and any report will be treated as confidential.

# RELTCO, Inc.

# DISASTER MANAGEMENT PLAN

**Effective Date 12/1/2016**

**Revised Date:2/15/17**

## *PURPOSE*

This Disaster Management Plan document is intended to provide information on the steps and procedures to be taken in the event of a manmade or naturally occurring emergency or disaster affecting the business operations of RELTCO, Inc. ("Company"). The Plan's purpose is to ensure the safety and well being of our employees and the orderly continuation of the Company's business, including the ability to service the needs of our customers with minimal disruption and delay. This document outlines the processes and procedures that will be implemented in the event of an emergency or disaster.

Different types of emergencies and disasters require varying degrees of response, from damage to a critical server; to a short-term, single site incident affecting our Company, only; to large scale, regional disasters of a relatively long duration affecting not only the Company but other businesses and governmental agencies in the area. This Plan cannot foresee and address all possibilities but is intended to address those risks the Company's management team believes to be most likely to occur and of greatest risk to the Company's operations.

We provide all employees with copies of this plan and any updates within [number of days] days of employment, and obtain signed acknowledgements of receipt for retention in their personnel files. We will practice the procedures outlined herein once a year and maintain a record of the date, participants and results of each training exercise.

# EMERGENCY RESPONSE TEAM

In the event of a disaster, or eminent emergency situation our emergency response team will be responsible for properly activating, and administering the Disaster Management Plan in conjunction with the Emergency Response Team Coordinator (note: in smaller agencies the same employee may perform overlapping functions)

**Emergency Response Team Coordinator**

The Emergency Response Team Coordinator is responsible for approving the Plan and updates to the Plan. In the event of an emergency, he/she has the sole authority to invoke and execute the Plan. The following person is the designated Emergency Response Team Plan Coordinator:

Paula Woodring
531 Isleworth Close
Tarpon Springs, FL 34688
727-239-1257
pwoodring@reltco.com
ppautauros@hotmail.com

In the event he/she is not available or is unable to respond to an emergency for any reason, the following person shall act in his place:

Delores Elftmann
1287 Overcash Dr, Dunedin FL 34698
727-483-9402 h
727-804-2331 c
delftmann@reltco.com
elftmann.delores@gmail.com

**Information Technology Coordinator**

Due to the Company's reliance on technology to efficiently operate its business, the following person has been assigned responsibility for assuring the redundancy of the company's computer and telecommunications systems to prevent the loss of data and provide for the restart of the Company's electronic communications capabilities within the timeframes specified herein:

Christopher Howell
11012 Oyster Bay
New Port Richey, FL 34654
727-364.7160
chowell@reltco.com
Text message

The IT coordinator will work directly with the Emergency Response Team Coordinator (or agency management) in planning the resumption of business services.

**Business Continuity Planning Team Members**

The members of this team are responsible for overseeing the deployment of this Plan within their area of responsibility

**Individual Contact Information Area of Responsibility**

Delores Elftmann
727-804-2331
Personnel

Christopher Howell
727-364.7160
IT

Mike DeFrancesco
727-612-5242
Client Contact

# EVACUATION ROUTINE

In the event of a natural or man-made disaster that necessitates evacuating our building such as fire or bomb threat, the following procedures will be followed:

**Declaration of Event and Order to Evacuate**
The Emergency Response Team Coordinator or, in his/her absence, the Alternate Emergency Response Team Coordinator will determine if an event has occurred that necessitates evacuation of the building. Once an event has been declared, the Emergency Response Team Coordinator will issue a warning and will then immediately contact the fire and/or police department.

**Warning**
A warning will be issued advising all occupants that there is an event requiring them to leave the building;

**Exiting the Building**
If instructions are given to evacuate the building, employees must use the stairs or fire escape to exit the building.

**Assembly Site:**
(Open grass field behind building if structure issues, main suite if weather issues)

**Reopening for Business**
Once the event is determined to be over the Emergency Response Team Coordinator will make the decision whether to reopen for business and allow employees back to their workplaces.

**Insurance Coverage:**
The Emergency Response Team Coordinator will determine if any damage to the building or operations occurred that may be covered under any of the Company's insurance policies.

# SHELTER IN BUILDING PLAN

In the event of a natural or man-made disaster that requires us to shelter within the building, such as a tornado or terrorist threat external to the building the following procedures will be followed:

**Declaration of Event and Order to Move to the Shelter Location:**
The Emergency Response Team Coordinator or, in his/her absence, the Alternate Emergency Response Team Coordinator will determine if an event has occurred that necessitates sheltering within the building. Once an event has been declared, the Emergency Response Team Coordinator will issue a warning and will contact the fire and/or police department if appropriate to do so.

**Warning**- A warning will be issued advising all occupants that there is an event requiring them to seek shelter;

**Shelter Location** – building location chosen to shelter in place. The basement or other secure location is recommended

**Note:** If the event is an earthquake, all employees are to immediately seek shelter under the nearest sturdy table or desk. If one is not nearby, crouch in the nearest corner using your arms to cover your head and face. Doorways should only be used for shelter if they are known to be in a supporting wall. Do not shelter near a window or other potential sources of broken glass.

**Reopening for Business**
Once the event is determined to be over the Emergency Response Team Coordinator will make the decision whether to reopen for business and allow employees back to their workplaces.

**Insurance Coverage:**
The Emergency Response Team Coordinator will determine if any damage to the building or operations occurred that may be covered under any of the Company's insurance policies.

# VITAL RECORDS PRESERVATION PLAN

This section of the Disaster Recovery Plan is designed for the protection and preservation of all vital information and critical data (including NPI), both in electronic and hard copy forms. This would include any important papers and / or files, as well as any vital information that is saved electronically. This operation will be coordinated with the Emergency Response Team Coordinator (or agency management) and the IT Coordinator.

Company data is backed up daily to a remote server located (onsite in server room and cloud also)

Physical files are maintained (in our office in a locked file room, or locked file cabinet)

Vital paper documents and files are scanned on a daily basis. Copies of the scanned documents are maintained on our with our daily backed up data maintained at on site and cloud also

Once a disaster is eminent and the Plan has been activated, the following procedures will be initiated:

**Electronic Data Processing**

The Emergency Response Team (ERT) will be informed of the existing situation and immediately begin the gathering, securing and transferring process to our off-site storage area

When possible, all computer hardware will be secured and prepared Christopher Howell and Vology for movement to emergency operations location determined at time of emergency.

If our computer hardware has been destroyed or become otherwise unusable, our IT Coordinator will immediately begin the process of restoring our system from the backup at Datto Cloud

**Vital Paper Files and Documents**

If possible, all important paper files will be included in the transfer to (our off site storage or emergency operations location). This includes copies of our insurance policies, banking information and a copy of our disaster recovery.

## TELEPHONE NUMBERS FOR EMPLOYEES, VENDORS AND CONTRACTORS

In the event there is a disaster (or that a disaster strike is eminent) below is the list of employee, vendor, and emergency personnel contact numbers. This will allow our Emergency Response Team Coordinator (or agency management) to properly and efficiently complete their respective responsibilities.

**Emergency Contacts**

Employee Contacts – see Best Practices Policy 3 Privacy and Information Security

Emergency Business Location 531 Isleworth Close Tarpon Springs, FL 34688 (or adjusted at time of emergency based on terrain conditions)

Local Police - 911 emergency non-emergency 813-247-8200 / Hillsborough County Sheriff's Office

Fire and Rescue - 911

Poison Control - 911

Utilities (electric, gas phone) TECO Electric/Gas – 813-275-3700, Hillsborough County Water – 813-272-6680

Title Insurance Underwriter Stewart Title & Guaranty – Liz DeQuesada 813-416-4913 / NATIC Geoffrey 305-310-5173Harris

Title Software Vendor / Resware 970-215-6249

Telephone Equipment ShoreTel 888-322-3822

Mail Services 813-908-2467

Alarm Services EEI 813-264-1907

Building Contractors/Management Company Saaba Development 813-843-4805

# PRIVACY NOTICE

**This Privacy Notice is provided on behalf of RELTCO, Inc.**

Congress passed the Gramm-Leach-Bliley (GLB) Act, which deals in part with how the financial services industry handles nonpublic personal financial information. RELTCO, Inc. recognizes that the foundation of our business is maintaining your trust and confidence. In order to provide you with the most effective and beneficial service, we must maintain information about you. Keeping that information secure and private is important to us. This notice is provided to you so that you may know how we collect information about you, the type of information we collect, what we may disclose to our affiliates and non-affiliated third parties, and the steps we take to protect personal information about you.

## What We Collect

First, we must collect a certain amount of personal information about you in order to provide customer service, offer new products or services, administer products, and fulfill legal and regulatory requirements. Therefore, as part of our servicing of your requests, we may obtain certain nonpublic personal information about you. This information includes facts and data that we receive from you, real estate agents, lenders, government agencies, and/or other authorized persons in varying manners, including but not limited to title orders, sales contracts, company required forms, telephone calls, correspondence, loan pay-offs, and other processing forms; facts and data about your transactions with us, our affiliates or others; and facts and data we receive from consumer reporting agencies.

## What We Share

RELTCO, Inc. is committed to maintaining the confidentiality of the personal information we collect. We welcome this opportunity to clarify our privacy policy for you.

## With respect to the information we collect about you:

- We collect and use the information to the extent needed to conduct our business and to meet our high quality service standards;
- We restrict access to the information to authorized individuals who need to know this information to provide services and products to you;
- We maintain appropriate safeguards to protect information about you;
- We will verify that any persons requesting information about you or your relationship with us is entitled to such information prior to providing it.
- We share nonpublic personal information about you outside our company only to service your request, or as authorized by you, or as required or permitted by applicable law;
- We require any organization that provides assistance to us in providing services on our behalf to you to maintain the confidentiality of nonpublic personal information about you and not use such information for any other purpose; and
- Our Privacy Policy does not allow non-affiliates to offer their products and services to you.

The law does permit us to share information about you with our affiliates, including insurance companies and insurance service providers. The law also permits us to share information about you with companies that perform marketing services for us, or other financial institutions that have joint marketing agreements with us. The information we share with our affiliates or service providers need not be directly related to our transaction with you.

If we change our privacy practices, we will provide you notice of all material changes. This privacy notice supersedes all previous notices with respect to matters described herein.

It is our goal to ensure that all the information we collect is accurate and complete. Please notify us if you believe information is inaccurate.

**A copy of our Privacy Policy is available on our website** www.reltco.com

**And a copy of our Privacy Policy is given at closing**

**No Action is Required By You**

You do not need to do anything as a result of this notice. It is meant to inform you of how we safeguard nonpublic personal information about you.

**We strive to maintain your confidence and trust.**

# RELTCO, Inc.

# SETTLEMENT, RECORDING & PRICING POLICY

**Effective Date 12/1/2016**

**Revised Date:**

## Best Practices Policy #4- Settlement, Recording, & Pricing

RELTCO, Inc. complies with Federal and State Consumer Financial Laws as applicable to the Settlement process. Compliance with the following procedures is required of all employees and failure to comply with the procedures outlined herein will be grounds for immediate termination of employment. We will conduct a quality control check of files to ensure that we are complying with our policy.

**A. Settlement Procedures.** To help ensure we can provide a safe and compliant settlement we will:

1. Follow all lenders' closing instructions.

2. Obtain a signed settlement/closing statement, disbursement statement, closing disclosure (CD) or other similar document that totals properly and is supported by written instructions for all amounts (i.e., closing instructions, invoices, written payoffs, etc.). This is to be included in each closing file.

3. Include in each closing file an accounting ledger/disbursement sheet that details all receipts (form of payment, date, and amount) and disbursements with date, transaction type, check number, payee, amount, and file's ending balance.

4. Agree all receipts and disbursements to the final signed settlement statement, disbursement statement, closing disclosure (CD) or other similar document.

5. Ensure all files balance to zero. If any balance remains, the date, reason for the balance, and to whom the balance belongs is to be clearly documented within the file.

6. Ensure all receipts are supported by a copy of the check, wire confirmation, or numbered cash receipt, and deposited prior to or on the day of closing/disbursement.

7. Make disbursements only after "good funds" (according to each state's requirements) have been established.

8. Ensure that all commitment requirements are satisfied.

9. Record all documents for the transaction (mortgages, deeds, releases, etc.) with the proper authority in a timely manner.

10. Maintain appropriate supporting documentation in all closing files, including, but not limited to the following

    - Valid identification of parties to the transaction
    - Properly executed affidavits, where required
    - Documentation that Privacy statement(s) were provided to the appropriate parties
    - Documentation that the Patriot Act requirements (review of the Sanctions List) have been met.
    - Compliance with FIRPTA requirements

11. Ensure any funds held after closing are held and disbursed in accordance with a formal escrow agreement executed by the appropriate parties. The agreement will include specific instructions as to when and how these funds are to be released.

**B. Pricing Procedures.** We have adopted the following procedures to help ensure all consumers are charged proper and appropriate rates for title insurance and appropriate amounts are remitted to our underwriters to comply with our contractual agreements.

1. For each title order received we will utilize the online rate calculator, or rate manual to ensure we charge the proper rate for all policies, endorsements and state specific fees as appropriate.

2. All applicable discounted rates will be charged including Reissue and Refinance rates for each transaction.

3. A printed copy or written record of all rate calculations will be kept in each file.

4. If we are notified of a rate change we will verify the change has been noted by our software provider and proper updates made to ensure the new rates are being utilized.

5. All appropriate personnel will be made aware of any rate or fee changes immediately to ensure consumers are always charged appropriate rates.

6. A quality check of our closed files will be periodically performed to verify consumers were charged proper rates and fees established by our company. Any overpayments will be promptly refunded to customers upon discovery and documentation maintained in the file.

**C. Recording procedures.** In order to ensure the timely and accurate recordation of all documents we will:

1. Ensure all documents are submitted or shipped for recording to the proper recording office within two business days of settlement, or receipt by us, if the Settlement is not performed by our company.

2. Track all documents shipped or sent for recording and we have verified that our software can generate a recording log for all documents and use the tracking system appropriately

3. Verify that documents were recorded and maintain recording information for each document in the individual file.

4. Begin corrective action on all rejected recordings within 2 days of receipt of the document. Notes will be maintained on the reason for the rejection and corrective action taken to resolve the problem. These re-submitted documents will be tracked and recordation information maintained in the recording log and file.

D. Oversight of Third Party Signing Professionals

1. We engage third party signing professionals (TPSP), including notaries public, as needed. We ensure that all TPSPs that we engage possess the appropriate qualifications, professionalism, and knowledge by maintaining a validation process and logging the information in the Third Party Signing Professional Tracking Log or notification is provided via email or phone call.

2. As part of the oversight process we:

a. Verify that the TPSP maintains an errors & omissions policy, and obtain a copy to ensure its' effective dates

b. Verify that the TPSP maintains a surety bond (if required), and obtain a copy

c. Verify and obtain a copy of their current state licensure, where required, or evidence that they have attained a recognized and verifiable industry designation

d. Obtain a Signed Service Provider agreement or train the TSPS to ensure that they are aware of the Company's obligation to protect NPI and they agree to do the same

3. In the event that a third-party signing professional is contractually retained by anyone other than the Company (including the buyer or seller), the responsibility for verifying that the third-party signing professional meets applicable standards rests with that party.

**Internal Monthly/Quarterly Quality Control Check of Recording, Pricing, & Refunds**

**Procedure: Conducted monthly at time of remittance reporting**

**(Data maintained on designated folder share drive)**

| File No. | Date Closed | Rate Charged | Rate determined by Quality Control Check | Recording Charged | Actual Amount to Record | Any overcharge was returned to customer (yes, no, n/a) |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Completed By: _____**

**Date:_____**

# Third Party Signing Professional (TPSP) Tracking Log

| Company/ Individual Name | E&O coverage through | Received copy of E&O | Received copy of surety bond, if required | Licensed through date | Received copy of License | Signed a Service Provider Agreement or has been trained in the Company's applicable policies |
|---|---|---|---|---|---|---|
| *Reltco Signing Portal Keeps current tracking, changing to TPSP 01/01/2017* | *01/01/2017* | *Yes* | *N/A* | *01/01/17* | *Yes* | *Yes* |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Maintain all copies of the errors & omission polices, bonds, and licenses or other applicable industry designation in a designated location, portal/file**

# RELTCO, Inc.

# TITLE POLICY PRODUCTION AND PREMIUM REMITTANCE

**Effective Date 12/1/2016**

**Revised Date:**

**Best Practices Policy #5: Production & Premium Remittance** RELTCO, Inc. meets its legal and contractual obligations for the production, delivery, and remittance of title insurance policies.

To help our agency meet our legal and contractual obligations to our underwriters, and ensure accurate production, and prompt receipt of the title policy by our customers, we have established the following procedures for title policy production and underwriter premium remittance.

**A. Title Production and Policy Delivery**

1 We issue and provide the policy to the customer within 30 days of the date of settlement, or 30 days from the date by which all the terms and conditions in the commitment were satisfied, maintain a confirmation of said delivery (email, fax, letter, etc).

**B. Premium Reporting and Remittance**

2 We report policies (including a copy of the policy, if required by the underwriter) to the underwriter by the last day of the month following the month in which the insured transaction was settled.

3 We remit premiums to underwriter no later than 45 days after the later of (i)the date of the Settlement, or (ii) the date that the terms and conditions of the title insurance commitment are satisfied.

# RELTCO, Inc.

## Insurance & Bond Coverage

**Effective Date 12/1/2016**
**Revised Date:**

**Best Practices Policy #6: Insurance & Bond Coverage:** RELTCO, Inc. maintains appropriate levels of professional liability insurance, errors and omissions insurance, and fidelity or surety bond coverage per state and underwriter requirements to help ensure our financial capacity to stand behind our professional services and in accordance with state law and title insurance underwriting agreements.

1. **Professional Liability or Errors and Omissions Insurance.** Our company maintains professional liability insurance in the amount of no less than $2,000,000.00. We determined this amount is appropriate given our company's size and complexity and the nature and scope of our operations; the amount is not less than the amount in our company's underwriting agreement(s). We review our coverage and endorsements on an annual basis to ensure it is still appropriate and reflects the type and nature of our current business.

2. **Fidelity Bond Coverage** Our company maintains a fidelity bond policy in an amount of not less than $___250,000.00. We have reviewed both state law and our Policy Issuing Agreement with our underwriters to verify that our coverage meets or exceeds their respective requirements.

3. **Surety Coverage** Our company possesses Surety Bond Coverage in an amount not less than $500,000.00_ as required by state law

# RELTCO, Inc.

# CONSUMER COMPLAINT HANDLING POLICY

**Effective Date 12/1/2016**

**Revised Date:**

**Best Practices Policy #7: Consumer Complaint Handling:** RELTCO, Inc. has instituted a process for receiving and addressing consumer complaints to help ensure reported instances of poor service or non-compliance do not go undiscovered.

This document describes the Complaint Handling Policy of RELTCO, Inc. (hereinafter the "Company") which has been implemented to ensure compliance with the laws and regulations relating to complaint handling. Compliance with the following procedures is required of all employees and failure to comply with the procedures outlined herein will be grounds for immediate termination of employment.

**A. Application.** This Policy applies to all employees and officers of the Company.

**B. Objective**. Our objective is to minimize damage to our reputation and reduce the risk of litigation by:

1. Handling Complaints from our customers in a timely, effective and consistent manner;
2. Recording Complaints in the Complaint Log; and
3. Periodically reviewing information in the Complaint Logs in an effort to identify trends or recurrences in order to take preemptive action to address the cause of such complaints.

**C. Person Responsible Delores Elftmann, Mike Pezone** are hereby designated as responsible for the application of this policy, and to review this policy on a regular basis to ensure that it continues to comply with industry laws, regulations, guidelines and best practices.

***Dino Avdic**, with back up **Paula Woodring*** are also responsible to communicate this firm's policy to all employees and officers of the Company.

**D. Definitions**

"Client" means an insured or any person acting on behalf of the insured; a regulator; or an agent of the Company.

"Company" means an employee or vendor of the Company.

"Complaint" will mean any written statement or verbal communication (phone call, voicemail, email, or regular mail) from a Client alleging a grievance involving the conduct, business, or affairs of the Company.

A complaint should include at least one of the three following elements:

- Complaint about the Company;
- Damages or potential damages suffered by the Client other than damages arising from matters insured under a policy of title insurance
- Request of corrective measures.

For greater certainty, errors that the Company accepted to correct are not considered as Complaints unless repetition or recurrence causes grievance to a Client.

**E. Complaint Log.** "Complaint Log" is a database to track key elements of the complaint process and category in order to identify potential trends or concerns and to produce reports.

**1**. All complaints must immediately be reported to **Delores Elftmann, Mike Pezone.**

**2**. All Complaints will be logged in the Complaint Log by **Delores Elftmann, Mike Pezone** The Complaint Log must, at a minimum, include the following information:

- Date of Complaint;
- Complainant's name;
- Nature of the Complaint and the circumstances;
- Name of the person who is the subject of the complaint;
- The product or the services which are subject of the Complaint; and
- The date and conclusions of the decision rendered in connection with the Complaint.
- The date the Complainant was notified of the resolution.

**3.** Each Complaint in the Complaint Log must be maintained for a period of seven (7) years, following the resolution date.

**F. Change of Procedures and Disciplinary Measures**

***Delores Elftmann, Mike Pezone*** must monitor the Complaint Log, record any corrective or disciplinary measures taken, if necessary, and provide recommendations for change in the Company's procedures, if appropriate.

# Complaint Log

**Complaint No._____**

| **CLIENT INFORMATION** | | | | |
|---|---|---|---|---|
| **Client Name** | | | | |
| **Phone No.** | | | | |
| **Address** | | | | |
| **Email address** | | | | |
| **Client reference no., if applicable** | | | | |
| **COMPLAINT INFORMATION** | | | | |
| **Date received** | | | | |
| **File or Policy reference no.** | | | | |
| **Nature of Complaint** | *Claims Handling* _____ | *Policy Issuance* _____ | *Closing* _____ | *Other* _____ |
| **Employee who is subject of complaint** | | | | |
| **Details** ***(I****nclude name of individual making Complaint if not the Client.)* | | | | |
| **Employee assigned to investigate** | | | | |
| **Date assigned** | | | | |
| **Date resolved** | | | | |
| **Resolution** ***(I****nclude name of employee who resolved this Complaint.)* | | | | |
| **Date Client notified of resolution** | | | | |

**AFFIDAVIT OF RECEIPT AND COMPLIANCE (to be signed by all employees)**

I acknowledge receipt of the following:

- Consumer Complaint Handling Policy

and agree, as a condition of continued employment by , RELTCO, Inc. to abide by and comply with the policies, procedures and requirements as set forth therein.

**All items can be obtained upon request**

**Personnel files are housed in HR office**