CENTRAL COLORADO TITLE & ESCROW

POLICIES AND PROCEDURES
COMPLIANCE WITH CFPB AND ALTA BEST PRACTICES
Created June 22, 2013
Last Updated: August 17, 2016

1. **Compliance with licensing requirements and applicable laws**
2. **Escrows/Funds/Accounts**
3. **Security and Privacy**
4. **Settlement Processes**
5. **Policy Production**
6. **Insurance Coverage**
7. **Consumer Complaints**

This policy manual forms a part of every contract for employment for any employee of the company, and any failure to follow the policies set forth herein is grounds for disciplinary action, including termination.

This policy manual (or any portion hereof) may be given to customers or clients upon request, including but not limited to as part of any lender compliance review or potential order request, but should be sent only in "non-writable" form through encrypted means in order to protect the Company's proprietary interest in this manual.

Recipients of a copy of this manual may only use the same for legitimate purposes related to the evaluation, vetting, or compliance review of the Company as part of the business relationship between the recipient and the Company, and acceptance of a copy of this manual shall constitute acknowledgement that this manual is proprietary to and is owned by the Company and may not be copied, modified, or used for any other purpose.

1. COMPLIANCE WITH LAW/MAINTENACE OF LICENSES

Personnel generally

We are a small company and our most important asset is our people and their relationships with our customers. We have always recognized this and are fortunate to be in an environment where we know each other and our backgrounds well and work closely together. With the institution of the CFPB, we now also running background checks (every three years) for all employees. Those particular reports are not available to third parties, but we do image results and store them electronically in a secure/protected environment, and we can certify or otherwise make evidence of having completed such searches available if required for audit purposes.

The Company's principals, who also manage the company hands-on and participate in the Company's day to day business, regularly engage in continuing education and training through ALTA, LTAC, First American, NAR, ROCC, ABA, CBA and other providers. Upon request, time off and reimbursement for training and education is generally made available to employees. In addition, when requested by the Company, employees will participate in training and educational seminars during regular work hours at the cost of the Company. Without limiting the foregoing, employees are regularly provided with opportunities for education and training, specifically including in the area of privacy and security and other Best Practices "pillars," and may be periodically required to participate in such training. Some of this training is through webinars and other online resources.

Licenses

All licenses required by the state of Colorado are in place and must be renewed as required by applicable regulations. The principals will review state licensing requirements and current staff licenses at least annually to ensure that all required licenses and any other desired licenses remain in full force and effect. Any employee holding a professional license must obtain the written consent of one of the principals of the Company prior to terminating that licensure or allowing a license to lapse. Any employee receiving any notice with respect to a license held by that employee shall immediately notify the principals of such notice and provide a copy of any written correspondence related to the notice or the license.

As of the date of the most recent update to this manual as stated on page 1:

4 employees hold title insurance producer licenses, 7 employees hold notary licenses, and the principals are attorneys who are and will continue to be licensed to practice law in the State of

Colorado. The Company also holds an ALTA Policy Forms License and is compliant with ALTA's licensing requirements.

The business entity is a registered limited liability company in good standing in the state of Colorado.

Copies of current licenses are stored in scanned form under the "Best Practices" Folder in the "Policies and Manuals" directory on the Company's "Z – drive", and copies may be shared, upon request, with customers, regulators, and others seeking confirmation of licensing for a valid business purpose.

Only employees holding a valid producer's license in Colorado may sell, negotiate or solicit title insurance business or sign policies, endorsements, O&Es or other title reports. Any employee desiring to become a licensed title insurance producer should review the licensing requirements available on the DORA website and raise the request with a principal. Paid time off and company funds for training/testing may be available and will be evaluated by Management on a case by case basis.

Other Legal Compliance Matters

The Company and each of its employees is and shall remain in compliance with all applicable state and federal laws and regulations applicable to the business of the Company, specifically including all current licensing and registration requirements. Gwendolyn C. Allen is responsible for reviewing, on at least an annual basis, laws specifically applicable to the title and/or settlement industry for updates, and for more generally monitoring laws and regulations applicable to small employers and to businesses similar to the Company. In the event management determines that changes to these Policies and Procedures are necessary or appropriate, whether to ensure compliance with any updates of such laws or otherwise, employees will promptly implement any such changes in accordance with instructions from management.

Specific Colorado Compliance Matters

The Company is regulated by the Colorado Division of Insurance and is and shall remain in compliance with the requirements of the Department of Regulatory Agencies, Division of Insurance, Title Insurance, 3 CCR 702-3-5-1. The Company is, and shall remain, in compliance with such regulations and with the requirements of the Title Insurance Code of Colorado (CRS 10-11-101, et. seq.) and with other applicable provisions of Title 10, Insurance, including without limitation those regarding:

*Reasonable Search and Examination Standards (*Note: *the Company is and shall remain in compliance with First American Title's Minimum Standards and Practices for Reasonable Search and Exam, the 12/7/12 publication of which is available on AgentNet and in pdf form in the "Best Practices" directory together with copies of the statutory requirements identified below)*

Regulations Relating to Title Updates, Policy Related Records, and Record Retention

Consumer Disclosure Requirements

Certification of Taxes Due

Rate Filings and Posting of Rates

Requirements for Policy Remittance

Employees who provide settlement services are required be familiar with the above referenced statutes and regulations, and are strongly encouraged to approach Management with any questions or concerns. Copies are available online and Gwendolyn C. Allen will provide a hard copy or pdf of any or all of the above statutes or regulations to any employee upon request.

The Company is also regulated in some respects by the Division of Real Estate, and employees are encouraged to familiarize themselves with the Colorado Real Estate Manual, which is available online at Colorado.gov through the Division of Real Estate portal.

2. ESCROWS/FUNDS/ACCOUNTS

Escrows Generally

We escrow funds when we accept earnest money, accept closing or settlement funds for disbursement at closing, agree to hold funds post-closing for any particular application and, in limited instances, when we open an escrow that is not related to a real estate or refinance closing. In the latter case, Management approval is required prior to accepting funds. Whenever we handle funds for any person or entity, we comply with all regulations and underwriting guidelines related to OFAC, including SDN searches.

Checks received for funds to be placed in escrow are generally deposited on the same business day, but in no event later than three business days following receipt, all in compliance with Division of Insurance Regulations (3 CCR 702-3). Funds received by wire are logged upon receipt of a wire confirmation and immediately associated with a particular open file. If the source of funds is unclear and the wire cannot be immediately associated with a file, the employee receiving the wire notice immediately advises one of the authorized signatories on the Company's escrow account to allow for prompt follow up.

Disbursements and closings are made only in accordance with good funds laws, which laws are summarized in our closing and escrow instructions.

All employees who accept a "Cashier's Check" as good funds must contact the issuing bank to confirm the availability of funds and the issuance by the bank of the check in question prior to disbursing any funds through the escrow based on such Cashier's Check. Similarly, if we receive wire transfer instructions in any manner that is unsecured (such as via non-encrypted email), the closer must contact (or cause another employee to contact) the financial institution or the party to receive such funds, as appropriate, to verify such wiring instructions. A notation must be made to the file as to the time and person making such verification.

In each instance where the Company accepts funds to be held in escrow, there must be written instructions for any actions taken or to be taken in connection with each such escrow. The standard form of Closing Instructions, together with the Company's form Addendum to Closing Instructions, cover earnest money and closing or settlement funds for real estate closings. However, any time we are asked to escrow funds other than earnest money and/or funds being delivered as part of a real estate purchase price or loan fees and any time we are asked to hold funds post-closing following a real estate sale (such as, without limitation, any escrows suggested for repair items or as a means to satisfy title requirements or to resolve title issues or inspection objections), one of the principals must be consulted and an Escrow Agreement must be included in the documents signed at Closing, or the Closing Instructions/Addendum must be modified as appropriate to specifically address the escrow. In all such cases, commencing November 15, 2015, following the Closing, the closer must update the "Post Closing Escrow Spreadsheet" to identify the file, the amount escrowed, the purpose of the escrow, and the anticipated timing of expected disbursement(s) and/or outside date under the escrow.

For document escrows (where original documents are being held on behalf of a third party following Closing), an Escrow Agreement should be executed wherever possible, and a note must be made in the file regarding such continued escrow. Any Promissory Notes or other negotiable instruments to be held by the Company must be held in the safety deposit box or in the fireproof safe and must be identified to one of the principals and also noted by the responsible closer on the "Note Inventory." The only promissory notes held in the fireproof safe should be those we are holding in temporarily while awaiting returned recordings or in anticipation of upcoming releases or partial releases; other promissory notes should be delivered to the safety deposit box(es) promptly in those instances where parties specifically request that we hold such items.

Accounts and Accounting

We maintain our escrow and trust account(s) separately from our operating accounts. Escrow funds are never commingled with operating or personal accounts. Appropriate identification (trust/escrow account) appear on all account related documentation, including bank statements, bank agreements, checks and deposit tickets. All accounts are maintained in Federally Insured Financial Institutions. No interest is earned for the benefit of the Company on funds in escrow or trust accounts. A spreadsheet of all accounts is maintained by Brett Eakins and is available on request for a valid business purpose. Wiring information for our Escrow Accounts is available on request for proper business purposes and can be found in the "Forms and Manuals" directory. Wiring instructions should be sent securely.

Financial transactions are conducted using authorized personnel only. *As of the most recent update to this Manual, t*he authorized signers on our account are Gwendolyn C. Allen and Brett W. Eakins, the co-owners of the Company, with Jennifer Leighton Scanga occasionally being granted temporary signing authority when the principals are both unavailable for a planned period of more than one business day. In addition, for certain of our front range closings, our remote closer, Ryan Rodenbeck, has signing authority for the related front range escrow account. Outside of business hours, checks are kept safely locked and inaccessible. We do not use electronic signatures or stamps to sign our Company's check stock.

In the event a check must be voided (due to misprint, incorrect information, late requests for cashier's checks, etc.), an authorized signatory must place the stop payment order, and appropriate notations will be made to the file, with the voided check being clearly marked, scanned/saved, and shredded (or converted to a cashier's check if applicable and delivered to the bank) after appropriate accounting measures are taken.

Wire transfer requests to our bank to disburse funds from a Company account must be signed by an authorized signer of the Company, following the closer's verification of wire instructions as appropriate as set forth above. Such requests are sent securely and require double verification from our banking institution. Federal reference numbers and other verification information is sent by the bank to the Company representative authorizing the wire and the Closer appends that information to the appropriate file.

Escrow Reconciliation/Register Review.

We maintain strict procedures and controls for escrow/trust accounts allowing for electronic verification of reconciliation. We utilize positive pay for our Escrow Accounts, and escrow reconciliations are available electronically to our underwriter(s). Reconciliation services are provided by a third party CPA, and all reconciliation is reviewed by Brett Eakins, principal and president of the Company, who also takes advantage of industry seminars, webinars, etc., as

suggested by Gwendolyn Allen, principal and compliance officer, to ensure we have the best information and are taking advantage of all available protections and resources.

The Company performs three-way reconciliation of escrow/trust account(s) on at least a monthly basis, and receipts and disbursements are reconciled daily, with two way reconciliation occurring within a business day of the transaction. Any exception items are resolved promptly following reconciliation, and reconciliation reports and supporting documentation are stored electronically to allow for prompt electronic verification. In the event the adjusted book and bank balances reveal bank fees or charges assessed, the applicable account is funded from an operating account within 30 days of completion of reconciliation.

The Company also performs periodic reviews of any checks going back into escrow, paid to cash or employees, transferred between accounts, suspicious payees, multiple checks to the same payees, and any other questionable disbursements. This review includes the following procedures:

1) Identify all outstanding checks.
2) Identify high-risk outstanding checks, such as:
    a. Recording, tax, flood/hazard insurance premium checks over 30 days
    b. Underwriter premium/payments that are outstanding over 60 days
    c. Any check over $5,000.00
3) Research to ensure outstanding check was disbursed properly; if yes, make immediate contact with the payee. If contact is unsuccessful, escalate to management for further direction.
4) Document the contact with the payee and result.
5) Research and update address information if required.
6) If response is received, void and reissue check to payee, or otherwise address as appropriate.

The Company also tracks outstanding file balances and will document any outstanding file balances over 180 days. Reports are periodically run (at least monthly) to show all outstanding checks, which are reviewed by management. Copies of written correspondence regarding uncashed checks or outstanding file balances are to be scanned and saved in the appropriate file.

Unclaimed Property/Uncashed Checks

In addition to the procedures regarding high risk checks stated above, at the end of each quarter, the Company will identify any checks issued by the Company that have not been cashed within six months of issuance and will attempt to contact the payee of the check to confirm that the payee has received the check and to encourage the payee to deposit or cash

the check. If a payee indicates that the check was lost, a stop payment order will be made and a replacement check sent as directed by the payee.

For any payees that cannot be reached, the principals shall monitor and ensure compliance with all state guidelines regarding unclaimed property and escheat.

In addition, the Company identifies, researches, and resolves the following significant items as applicable:

1) Outstanding balances over $10,000 over 10 days old

2) Outstanding mortgage payoffs over 10 days old

3) Escrow Trust Account with aggregate short over $10,0000

An explanation for any such outstanding file balance will be documented and updated at least monthly, and Management will follow up as appropriate to resolve such matters.

3. SECURITY AND PRIVACY

GENERALLY

The Company has an established culture of professionalism, trust, and integrity, and this policy derives from and is intended to reinforce the Company's commitment to protecting the Company's customers, clients, and employees. Discretion, integrity, honesty and trust are each a given within our Company, but exterior challenges necessitate this particular policy, which is specifically designed to protect the non-public personal information of our customers and clients ("NPI") as well as the Company's Confidential Information and Internal Use Only information, as each such term is defined below, all consistent with ALTA Best Practices and CFPB guidelines and requirements.

Employees have a critical role in properly securing data and ensuring the continued privacy of our clients, and this responsibility is taken seriously. Employees also recognize that information is a valuable asset of the Company and that data and information security is a critical component to ensure the confidentiality, integrity, and reliability of that information. This policy establishes the minimum requirements necessary to protect information assets against unauthorized access, modification or destruction.

For purposes of this policy, "**NPI"** means: Non-public Personal Information, which is any data or information considered to be personal in nature and not subject to public availability as defined by the Gramm-Leach-Bliley Act ("GLB Act") of 1999, such as loan/account numbers, social security numbers, and copies of drivers' licenses; **"Confidential Information"** includes but is not limited to company private lists and databases, customer lists, contact lists, research data, trade secrets, corporate strategies, and other information that is competitor sensitive. **Internal Use Only** means information for Company employees (e.g. internal email messages, company intranet, internal policy/procedure, training materials, employee performance evaluations, employee notes, computer passwords, and company financials). Employees shall take all necessary steps to prevent unauthorized access to NPI, Internal Use Only, and Confidential Information.

The Company has established an Information Security Risk Assessment that ranks risks including locations, systems and methods for storing, processing, transmitting, and disposing of NPI. Procedures used by management in this regard are attached as **Addendum I.**

All policies are reviewed and updated as appropriate, but given the nature of technology, employees should understand that this policy in particular is subject to adjustment and change as needed. The Company continually reviews operations to identify and assess external and internal risks to security and our ability to maintain the confidentiality and privacy of NPI. Employee feedback is especially welcome in this regard. Employees must also immediately report any perceived or actual violation of this policy and/or threat to the security or privacy of any NPI to Gwen Allen. Gwen has been appointed as the employee responsible for review of

and recommendations regarding changes to this information security and privacy policy. Any exceptions to the policies set forth herein must be approved by Gwen Allen or Brett Eakins.

As part of our Company's dedication to protection of our customers' privacy, and our commitment to compliance with disaster recovery policies, commencing on January 1, 2015, we are taking advantage of electronic protection and storage. All files opened after such date are completely paperless following policy issuance, and even prior to shredding the paper file all NPI is digitally entered when received and promptly shredded rather than being stored in active paper files. We have also taken advantage of available insurance coverages for cyberfraud/data protection as noted in the insurance section of this manual.

Our title production software and cloud based secure electronic storage is provided through one of the largest most reputable companies available, SoftPro (through their Hosted Select environment), which is also an American Land Title Association ("ALTA") approved vendor compliant with ALTA Best Practices. Technological specifications related to their privacy protections can be obtained from SoftPro upon request.

With respect to active files and older files for which we are not yet equipped to convert to paperless storage, we maintain a clean desk policy, such that each employee must:

1) Close paper and/or electronic files containing NPI when they are away from their desk.

2) Log-off or lock their computers when unattended for an extended period.

3) Enable a password-protected screen saver.

4) At the end of each working day, safeguard any documents, files, portable devices, and electronic media containing NPI, noting that NPI should be digitally stored and then paper copies shredded as soon as possible rather than being left in active paper files.

5) Secure all keys used to access NPI.

6) Remove all documents containing any NPI from any copier/fax machine

7) Secure passwords at all times.

Management consistently supervises office practices and periodically engages in evaluations to ensure compliance with the above procedure.

On those occasions when we are required to forward documents containing NPI to a customer or lender, we use "ShareFile" encryption services for any electronic correspondence, and will fax the document(s) when the legitimate recipient is unable or unwilling to use the secure link. Where lenders request, we will upload such information to the lenders' site(s) based on the lender(s)' representations that such site(s) are secure.

We are a small company with very few third party service providers who have access to our office or to our data. We take all reasonable steps to select and retain service providers that are capable of appropriately safeguarding NPI, including those detailed on Addendum S attached hereto. Those service providers (*As of the last update to this Manual – those are only IT and copier/scanner providers)*, are subject to nondisclosure agreements and have been fully vetted as appropriate. More information regarding those providers is available upon request.

Review of security controls is conducted at least annually.

PHYSICAL SECURITY

The Company is the sole occupant of our building, which is locked and secure outside of business hours. During business hours, there is a single point of entry for customers and service providers, which is physically manned by a staff member.

As previously noted, for all files commencing with those opened January 1, 2015, all NPI is scanned and stored via SoftPro upon receipt. Documents containing NPI are separately scanned and labeled as such or by document title, and are shared only with the party whose information is contained in such documents or their lender, or at such party's direction. Physical files are shredded upon policy issuance or cancellation of the transaction. The Company currently uses a licensed provider with the name of "Shred It" to dispose of shredded materials. Older physical files are stored in a separate location that is closed off and secured when not in use, and only responsible employees have access to the content of those files.

Employees may not give anyone a "copy" of their file or allow them to take a full file into one of our conference rooms. Rather, if someone asks to look at "their file," the employee taking the request should obtain a more specific identification of what is needed and copy only the relevant information, ensuring that NPI and Confidential Information has been excluded or redacted.

The Company retains records in compliance with all legal and contractual requirements. Because our data is a significant asset of our Company, we do not destroy data/files after legal compliance period expire. Rather, such information is securely stored as described in this policy.

COMPUTER, INFORMATION TECHNOLOGY AND SYSTEMS SECURITY AND USE

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of The Company. These systems are to be used solely for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment and systems, software, networks, and internet at the Company. Employees understand and acknowledge that inappropriate use may expose our customers and clients to risks and also exposes the Company and our systems to risks, including virus attacks, compromise of network systems and services, and legal issues.

While the Company's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the Company's systems remains the property of the Company and equipment, systems and network traffic are subject to monitoring by the Company.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of stated policies, employees should be guided by good judgment, and if there is any uncertainty, employees should consult their supervisor or manager. Under no circumstances is an employee of the Company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Company-owned resources. In addition, and without limiting the generality of the foregoing, the activities described in Addendum Z, entitled "Unacceptable Use" are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Employees must use extreme caution when opening e-mail attachments received from unknown senders and employees are not permitted to install, download or remove software without prior approval from management, except as necessary for compliance with the TRID requirements of known lender customers. Users may download/log-in to lender systems as required by known lenders to accommodate compliance with lender requirements, CDF production and access to closing documents and figures.

LOGICAL ACCESS

The Company restricts access to NPI to those employees who need to know that information to provide products or services to customers. The Company maintains physical, electronic, and procedural safeguards that comply with federal regulations to guard NPI.

Each employee is required to have a unique User ID and password which is not shared. The User ID will be permanently decommissioned when no longer required. Appropriate access levels and permissions are based on job role and responsibility and on business need.

Security controls (e.g. password protection, encryption) for physical media, electronic media (e.g. email, database access) and wireless devices are also used to prevent unauthorized access,

misuse, or corruption of NPI while in transit. Removable Media containing NPI is not permitted without prior written approval from Management. Upon such approval, it is the individual's responsibility to protect the Removable Media in their possession from theft or unauthorized access. Security controls (e.g. password protection, encryption) for Removable Media are used to prevent unauthorized access, misuse, or corruption of NPI while in transit. Employees are instructed not to leave documents or Removable Media containing NPI in a location (unlocked vehicle, hotel room) accessible to others.

In the event of the theft or loss of any laptop or supported media device through which Company information has been accessed, whether or not the device is owned by the Company, the employee shall immediately report the theft or loss to Gwen Allen, and appropriate action will be taken in conjunction with the Company's third party IT professionals.

The Company's network systems and firewall are configured to detect and log intrusion events, and alert appropriate individuals. Backups are made and maintained for all critical systems and data. Company systems are configured to record the User ID of persons who access the system. Anti-virus software is installed, functioning and maintained on servers, users' workstations, and laptops. Anti-virus is configured to scan external media as applicable. Employees other than system administrators are not permitted to disable anti-virus software.

Remote access (e.g. Virtual Private Network, "VPN") requires authentication to Company networks based on job roles and responsibilities and business need.

The Company maintains security authentication (e.g. password) to secure computers and other office equipment that contains or provides access to NPI. Access system requires passwords that are at least six or more alphanumeric and special characters, and do not contain common words, User ID, first or last name. Employees must keep passwords secure. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended. Employees are required to report any instance of compromised passwords and to change possibly compromised passwords immediately.

Company equipment and devices, keys, material, hardware and software, Removable Media and any documents will be returned upon termination of employment or contract. User accounts and network access including remote access will be immediately disabled for terminated Employees.

CUSTOMER PRIVACY POLICY

The Company provides its Customer Privacy Policy to its customers as required by law. Proof of notification to customer is retained by the Company. The Customer Privacy Policy is accessible by customers through the Company website. On an annual basis or as necessary based on

change in operations, legal and regulatory requirements, industry best practices, and available technology, management reviews, updates and approves the Customer Privacy Policy. If exceptions to the Policy are necessary, that request will be evaluated by Gwen Allen, the individual responsible for the Customer Privacy Policy. Any approved exceptions will be documented and recorded. *As of the most recent update to this Manual,* the Company utilizes FirstAmerican's privacy policy as the Company's own Customer Privacy Policy as well.

DATA BREACH AND DISASTER RECOVERY PROTOCOL, INCLUDING BUSINESS CONTINUITY

The Company's policies and practices are specifically formulated to minimize the risk of data breach, and the Company has also elected to obtain insurance against those risks where possible. However, the Company recognizes that in the current technological environment, there remains some risk of breach, and the Company also recognizes that the risk of physical disaster cannot be completely mitigated through these policies and practices. In the unlikely event of a data breach or of such a disaster, the Company will follow the guidelines set forth in Addendum D to this Manual.

Our use of a hosted solution title production software for data entry and file storage ensures that any disaster or breach of our systems or facilities will not result in an interruption of business. More information about SoftPro, which is a premier provider approved by American Land Title Association for Best Practices compliance, can be obtained upon request. Like all modern businesses, we are at risk for temporary internet interruptions resulting in short term business interruptions, but in order to minimize that risk we maintain an automatically triggered backup internet provider in the event our primary provider's service is not available.

4. SETTLEMENT PROCESSES

A. PRICING PROCEDURES AND CONSUMER FINANCIAL LAWS

Title Insurance rates are calculated and charged in accordance with the underwriter's rate manual. Documentation of any rate quoted must be included in the file (if any) opened for the transaction at issue, but use of SoftPro's rate calculation fields and/or AgentNet/360 integration is sufficient to satisfy this requirement. Employees are required to use either SoftPro or the 360/AgentNet integration for rate calculation for any active file, and to specifically note in the file any manual change or entry regarding rate calculation and the reason therefor. If assumptions are made in connection with such calculations, those should be noted to the file as well.

In order to ensure that appropriate reissue rate discounts are automatically applied when available, the title searcher or the employee processing the order must check to see if we have a "prior" on the property and, if not, must inquire with the person placing the order if a policy has been issued within the past 5 years (10 years for commercial transactions). If we have a prior policy issued within that time frame, or if a party can provide a copy of a policy issued within that time frame, reissue rates will automatically be applied.

The underwriter's rate manual must be available, in sight, in the lobby, for reference by customers and potential customers upon request. If estimated fees are requested of an employee, such rates and fees are also available through AgentNet.

Closing/escrow rates and fees for the Company have been updated through a rate filing with the State of Colorado's Division of insurance effective as of May 1, 2015. A summary of such fees is available in the "Forms and Manuals" directory.

The Closer or person responsible for preparing the Settlement Statement for a given transaction must double check that the amount charged is consistent with the Commitment and with the rate filing. The title examiner issuing the policy will also confirm that the rate charged was consistent with the Commitment and, if not, will report the error to management. In the event of any excess charge or overcollection, the party making the payment will be refunded promptly following Closing.

B. RECORDING PRACTICES

Whenever possible, recordings must be delivered to the appropriate clerk and recorder within 24 hours of closing. If for any reason a document has been signed and is to be recorded but is being held post-closing, management should be consulted and an escrow agreement may be required (see above regarding document escrows).

All documents should be copied or scanned and uploaded to the electronic file before being delivered for recording. Documents to be recorded in Chaffee County are collected and hand delivered once each business day. Documents to be recorded in other counties should be e-recorded wherever practicable but may be mailed/delivered in a manner which is "trackable" (such as UPS 2nd day or certified mail), if a record of when such mailing was sent is retained and a deadline set for the employee sending the recording to check on actual recordation or return of the recorded document by such county. Electronic recording is available in most Colorado jurisdictions, and will be utilized when available outside of Colorado if the parties are willing to pay charges associated with e-recording as part of the Settlement disbursements. Management will continue to monitor and evaluate the availability and cost of e-recording in Colorado counties other than Chaffee County.

If a recording is rejected by the County, for any reason, appropriate information should be scanned and noted in the file, and necessary corrections must be made and returned to the County as quickly as practicable. If the rejection results from an error of the data entry personnel, the document preparer or the Closer that either necessitates a scrivener's affidavit or requires contact with any of the parties, management should be consulted before any such affidavit is filed or any party (or agent of the party) is contacted with respect to the error or its correction.

Upon receipt of recorded originals, they should be sent in a timely manner to the grantee, with a copy retained in the closing file.

5. TITLE POLICY PRODUCTION, DELIVERY, REPORTING AND PREMIUM REMITTANCE

The Company does, and will continue to, remit premiums and issue title insurance policies to customers in a timely manner following closing, and in no event are policies delivered later than required pursuant to applicable law, contractual obligations, and/or underwriting requirements.

Commencing with files opened on or after October 1, 2015, if the Company handles the Closing, then (a) whenever possible title insurance policies are issued within thirty days, but in all events within sixty days, of final settlement; and (b) premiums are remitted and policies are reported to the underwriter by the last day of the month following the month in which the relevant transaction is closed.

For Closings which are NOT handled by the Company, then within 30 days of the Company's being notified of satisfaction of the Commitment's terms and conditions, the Company will prepare and deliver to the customer all title insurance products according to requirements in file instructions (e.g. lender instruction, escrow instructions).

The Company uses SoftPro 360 and "AgentNet" to ensure that policies are remitted, issued, and receipt of policy data is confirmed, in a manner calculated to ensure compliance with law, underwriting guidelines, and contractual obligations and in a manner calculated to avoid rekeying and errors.

Delivery of title insurance products is completed promptly following policy production and each file has an auditable trail regarding who sent the title products by 1 of the following 4 methods below:

1. **By email**:
    a. Original title insurance products are sent to the customer by email with a record of who sent the email, what product was sent, when, and to which email address;

2. **By US Mail**:
    a. Prepare paper originals with original policy jackets.
    b. Prepare appropriate envelopes with verified postal addresses.
    c. Scan and upload to the file a copy of the transmittal letter, and add a "Note" to the electronic file as to when the policy was sent.
    d. Place in US Mail with correct postage; or

3. **By Courier (FedEx/UPS):**
    a. Prepare paper originals with original policy jackets.
    b. Prepare appropriate air bills with verified physical delivery addresses.
    c. Scan and upload to the file a copy of the transmittal letter, and add a "Note" to the electronic file as to when the policy was sent.
    d. Place in correct box for pickup/drop off.
    e. Scan copy of air bill to file for file tracking.

4. **In Person:**
    Original title insurance products are given to a customer.

Commencing January 1, 2016, once per month, a review is undertaken or a report is generated to determine if title insurance policies have been issued for all files having a settlement date more than thirty days prior to the review date. If not, the responsible party will review and follow up with appropriate parties. Once all requirements are met or the Company has otherwise committed to issue a policy, title insurance products will be issued promptly. In the

event files consistently exceed the stated time frames in this procedure, Management will take appropriate remediation steps to reduce the backlog.

6. BUSINESS INSURANCE COVERAGES

Our coverages well exceed, and will continue to exceed, any legal requirements. The Company has affirmatively elected to purchase coverages not required by law in order to provide better protection and assurances to our customers and clients. The particular insurance coverages held by the Company are reevaluated at least annually to ensure that the policies held cover the risks inherent in the business of title insurance, escrow, and third party settlement services (from order through closing and beyond) and that such coverages are appropriate for the particular business of the Company.

The Company carries Errors & Omissions insurance and is covered by a Fidelity Bond. The Company also carries CyberLiability and Data Breach Insurance. Declarations pages for insurance policies are available in the legal compliance and insurance subdirectory of the "Forms and Manuals" directory.

7. CUSTOMER COMPLAINTS

Customer service is critical to our relationships and therefore to our business, and the Company prides itself on its dedication to positive relationships with clients and customers. Our reputation and our success are built on the trust of our customers. Employees are hired/retained in large part based upon a demonstrated ability to adhere to the highest standards of professionalism and client service, and employees are expected to perform with the utmost discretion and to always interact with customers in a way that is friendly but professional and that is respectful, courteous, trustworthy, responsive and reliable. We rarely receive complaints, but on those occasions when a complaint is raised, it must be resolved pleasantly and efficiently, and in a timely manner.

A "complaint" is any expression of dissatisfaction submitted by or on behalf of a customer of the Company. If a complaint is received in writing, it must be immediately handed over to one of the principals. If a complaint is left on a voice mail, the substance of the voice mail should be communicated as quickly as possible to one of the principals. If a complaint is made orally, whether on the phone or in person, the employee hearing the complaint should be sure to obtain full contact information from the complainant and should encourage the customer to speak directly to one of the principals, and the employee should report the substance of the complaint to one of the principals immediately. Employees may assure customers that one of the principals will get back to them within a business day of the day the complaint is raised. Oral complaints should stay at the oral level if at all possible. Do not advise a client to put their concerns in writing unless instructed to do so by a principal. Whether reported orally or in

writing, the report of the complaint should include as much background and specific information as possible, including the contact information of the complainant and the file number to which the complaint refers, if any. The Company will continue to monitor customer service levels and particular complaints and, if the Company determines that a written Complaint Intake Form is necessary or advisable, the Company will provide such a form to its employees for use in reporting complaints.

Written complaints will be kept in a complaints file, which file shall include all correspondence related to the complaint and documentation of its resolution, for at least three years from the date of the complaint.

Gwen Allen is designated as the point of contact for all complaints and will respond to complaints directly unless availability constraints make Brett Eakins better able to respond directly. If Gwen Allen is the subject of the complaint, it will be referred to Brett Eakins.

ADDENDUM Z – UNACCEPTABLE USE

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Company.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Company or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Known introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any Company account.

8. Making statements about warranty of the Company's work.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to Management is made.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, Company employees to parties outside the Company, except as required for vendor verification purposes or as otherwise approved by Management.

Email and Communications Activities

1. Sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within the Company's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Company or connected via the Company's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

MISCELLANEOUS

Postings by employees from a company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless posting is in the course of business duties. The Company reserves the

right to remove any Internet posting by an Applicable Party that is deemed inappropriate and/or damaging to the Company's reputation.

All hosts used by the employee that are connected to the Company Internet/Intranet/Extranet, whether owned by the employee or the Company, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

BLOGGING

1. Blogging by employees, whether using the Company's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the Company's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the Company's policy, is not detrimental to the Company's best interests, and does not interfere with an employee's regular work duties. Blogging from the Company's systems is also subject to monitoring.

2. The Company's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the Company and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the Company's Non-Discrimination and Anti-Harassment policy.

4. Employees may also not attribute personal statements, opinions or beliefs to the Company when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the Company. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the Company's trademarks, logos and any other the Company intellectual property may also not be used in connection with any blogging activity

ADDENDUM I - RISK IDENTIFICATION AND ASSESSMENT PROCEDURES

We have completed the following as part of our Risk Evaluation and Implementation of Controls:

1) Identify and prioritize risks associated with the protection of NPI. These risks are evaluated by:
    a. The impact and likelihood of an occurrence
    b. Estimated costs and impact if an event actually occurred
    c. Evaluation of the priority based on the impact, likelihood, costs and other important factors
    d. Location of NPI (onsite and offsite)
    e. Access by Applicable Parties

2) Implement controls to mitigate risks where appropriate (e.g., electronic storage a secure sending of NPI as discussed in Privacy and Security Policy section of Manual).

Risk Assessment Testing:

1) Risk Assessment is tested annually by Management.

2) In the event we discover any exceptions and/or control gaps, Management will detail those on Risk Assessment Worksheet, after which Management will evaluate and respond to such matters, including designation of a specific timeframe for remediation.

Any exceptions and/or control gaps will be remediated by one of the following methods:

a. Reduce or eliminate the risk.

b. Changes are made to procedures as applicable based on the risks perceived, scope and types of activities, and access to NPI.

A risk assessment review will be undertaken at least annually by Management, including, but not limited to, an evaluation of information systems, including network and software design; information processing, storage and disposal; detecting, preventing and responding to attacks, intrusions or other system failures.

ADDENDUM D

DATA BREACH AND DISASTER RECOVERY

DATA BREACH PROCEDURE

The Company has designated a responsible individual as the Data Breach contact for implementing this procedure.

1) **Monitor**:
    a. Deviation from policies, procedures or misuse of information and information systems will be monitored.
    b. All breaches of information security or loss of any device, actual or suspected, must be reported and will be investigated by the Data Breach contact.
    c. To the extent monitoring is being conducted by a Service Provider, Service Provider shall agree to follow Data Breach Incident procedure.

2) **Investigate**:
    a. Data Breach contact determines impact of incident.
    b. Data Breach contact analyzes and preserves log information.

3) **Respond**:
    a. Data Breach contact notifies Company management
    b. Customers and law enforcement will be notified of any Data Breach in accordance with applicable legal and regulatory requirements and the Customer Privacy Policy.

4) **Process Improvement & Remediate**:
    a. System and processes are updated to prevent further intrusion as applicable.
    b. Any delays in breach notifications will be documented by the Data Breach contact.
    c. Execute remediation as applicable (e.g. employee access restricted).
    d. Disciplinary action against Employees will be taken as appropriate.

BUSINESS CONTINUITY AND DISASTER RECOVERY PROTOCOL

A Business Continuity and Disaster Recovery plan is in place to protect critical business processes from effects of failures or disasters. This plan ensures secure methods to protect Company information and the timely resumption of business information systems. Our steps are to:

1) Identify and prioritize critical business components.
    a. Physical Offices

b. Equipment
c. Applications and services
d. Network
e. Telecom
f. Loss of critical Service Providers

2) Identify risks to critical business components.
    a. Environmental (*e.g. fire, flood, storm*)
    b. Technological (*e.g. hard drive failure, loss of internet*)
    c. Vandalism (*e.g. malicious computer attack*)

3) Identify timely restoration and alternative workarounds for each critical business components.
    a. Scheduled tasks to be completed
    b. Owner of scheduled tasks
    c. Application and services to be recovered

4) Identify individuals to institute workaround including contact information.

5) Backups are made and maintained for all data including offsite and secure locations.

6) Recovery of systems and data must be tested periodically to ensure that processes and procedures are effective.

7) Results of testing are documented on the Tracking Log.

ADDENDUM S

Service Providers

Select - Prior to selection of Service Providers, due diligence will be required such as an evaluation of their security policies, background screening on staff, financial viability, insurance coverages, references and disaster recovery plans. Due diligence materials are retained.

Verify- The contract provisions, service level agreements and non-disclosure agreements between the Company and the Service Providers will be in accordance with the Company's Information Security and Privacy Policy. The contract and agreements provide appropriate remedies for violations.

Implement- Service Providers will implement appropriate security controls in accordance with the objectives of the Company's Information Security and Privacy Policy.

Monitor - Where Service Providers are subject to expanded safeguards as applicable by regulatory, legislative or contractual obligations, the Company will monitor those expanded safeguards.

a. *The Company designates an employee as the Service Provider contact.*
b. *The Company Service Provider contact monitors performance on a regular basis.*
c. *If contract provisions, service level agreements or non-disclosure agreements are violated, the Company Service Provider contact takes appropriate action.*