ALTA BEST PRACTICES MANUAL

Supporting Documentation to Address Regulatory Compliance Guidelines for the: Consumer Financial Protection Bureau through ALTA's Best Practice Framework "Title Insurance and Settlement Company Best Practices"
Shield Title AZ

Shield Title AZ
2600 N. 44th St. Phoenix, AZ 85008 STE 103
(602) 848-2560

Mission Statement

This Best Practices Manual has been developed by Shield Title AZ in accordance with guidelines set forth by the American Land Title Association and in compliance with both the Gramm-Leach Bliley Act and the Consumer Financial Protection Bureau established under the Dodd-Frank Act. The goal of this manual is to outline the policies and procedures set by Shield Title AZ in our commitment to protect the security of the consumers and continue to provide professional quality service to our clients.

Introduction

Shield Title AZ's Best Practices Manual follows the guidelines of the American Land Title Association which was developed in order to "to help members illustrate to consumers and clients the industry's professionalism and best practices to ensure a positive and compliant real estate settlement experience." The compilation of this manual draws from previously designed policies and procedures active with Shield Title AZ including our Information Security Manual. In further compliance with the new regulatory environment, Shield Title AZ is also an approved settlement agent with Secure Settlements, Inc.

American Land Title Association (ALTA) has created "best practices" that are intended to define a set of strong procedures that the title insurance and settlement companies can follow to protect consumer information and provide higher levels of efficiency. The framework of ALTA's "best practices" is designed with the expectation that a strong foundation will be established through adherence to the seven distinct pillars outlined in this manual.

The "best practices" of an industry are methods and techniques that are proven to produce superior results in achieving higher benchmarks. The purpose is to maintain consistent quality that serves as an enhancement to mandatory legislated standards and promote the industries adherence to compliance.

ISSUED AND APPROVED: _____

Dated July 2022

By: Omar Qader, President

BEST PRACTICE ONE (1) - LICENSING

Definition: ***Establish and maintain current license(s) as required to conduct the business of title insurance and settlement services.***

Shield Title AZ Policy and Procedures: We maintain all local, state and national required business and insurance licenses. All title insurance licenses are tracked maintained through the Administrative Department. Established in 2022, Shield Title AZ is active and in good standing in Arizona. Copies of current insurance licensing is available in Appendix A.

- Licenses are renewed based on state regulations and at the earliest point that renewal becomes available.
- Annual Reports are filed and completed yearly with all applicable fees.
- Where applicable, continuing education credits are completed for agent licensing.

1.2 – TITLE INSURANCE LICENSE RENEWAL PROCEDURES

The state of Arizona issued the current Title Insurance Agency (Producer) License #3001790092 to Shield Title AZ on 02/15/2022. The expiration date for the current license is 05/31/2025. The Company is currently an authorized agent for ATGF (Attorneys Title Guarantee Fund, Inc.

ANNUAL PROCEDURES

The Company President reviews and determines state licensing requirements annually. The Company President maintains a License Log and current copies of all state required licenses in a single location along with evidence that the Company and its employees are compliant with current licensing requirements.

1. The Company President determines the states in which the company conducts the business of title insurance and settlement services. Presently, Arizona is the only state we operate.

2. The Company President reviews the insurance licensing laws for states listed above annually and determines the business and individual licenses that are required. A Title License Log is then created and maintained by the Company President for the next twelve months.

3. The Company President obtains copies of all business and individual licenses listed on the Title License Log and maintains them in a folder with the Title License Log. The details of each license are entered onto the Title License Log (including name, license #, expiration date and CE requirements).

4. The Company President confirms the current appointment of the Company and each individual on the licensing log with the title insurance underwriter(s) that the company has an agency contract with.

MONTHLY PROCEDURES

1. The Company President reviews the Title License Log monthly to determine if any licenses are due for renewal within the next 30-60 days and to determine if any individuals need to take classes to ensure compliance with Continuing Education (CE) requirements.

2. The Company President ensures that individuals that are not yet compliant with CE requirements for licensing period have plans to attend classes that will fulfill requirements prior to expiration date.

3. The Company President applies for renewal of all licenses no later than 30 days prior to the current expiration dates shown on the Licensing Log.

4. The Company President obtains copies of renewal licenses and places them in the Licenses folder.

5. The Company President notifies its underwriter(s) of any individuals or entities that should no longer be appointed.

Supporting Documentation: Copies of insurance licenses.

1.3 – NOTARY LICENSE RENEWAL PROCEDURES

Shield Title AZ ("the Company") shall only use currently licensed Notary Publics when Notary Public services are required in the conduct of the business of title insurance and settlement services.

The Company currently employs licensed Notary Publics who are utilized when Notary Public services are required.

1. A Notary Public License Log is maintained by the Company President for all commissioned Notary Publics that are employees of the Company. Copies of the licenses are maintained in a secure folder with the Log in the Company President's office.

2. The Company President reviews the Log monthly to determine if any licenses are due for renewal within the next 30-60 days and coordinate the notary license renewal with the individual licensee.

3. The Company President ensures all necessary renewals are applied for no later than 30 days prior to the current expiration dates shown on the Log.

4. The Company President obtains copies of renewal licenses and places them in a secure folder with the Log.

5. If for any reason a Notary Public other than one employed by the Company is utilized due to circumstances beyond the Company's control, the Notary Public's current license is verified by

researching the applicable state Notary verification website/database. Documentation of the Notary Public's license is maintained in the applicable settlement file.

1.4 – ALTA POLICY FORMS LICENSE RENEWAL

Shield Title AZ ("the Company") shall comply with the American Land Title Association (ALTA) requirement that all issuing agents of title insurance maintain a Policy Forms License or an Occasional Use Waiver. Shield Title AZ is a current member of ALTA.

ANNUAL PROCEDURES

1. The Company President shall determine if the Company will remain current dues paying member of the American Land Title Association (ALTA). If it does, the Company President will obtain a copy of the ALTA Membership Certificate and maintain it in a secure file in their office. An ALTA policy forms license is included with ALTA membership so the ALTA Membership Certificate is evidence of the Company's policy forms license.

2. If the Company is not a current dues paying member of ALTA, the Company President shall determine if the Company is eligible for an ALTA Occasional Use Waiver (issued less than 50 title insurance policies in the previous calendar year). If the Company is eligible for the Waiver, the Company President shall apply for one and once received maintain a copy of it in a secure file in their office.

3. If the Company is not eligible for an Occasional Use Waiver (issued more than 50 title insurance policies in the previous calendar year), the Company President will either 1) apply for an ALTA membership or 2) apply for an ALTA Policy Forms License. Once the ALTA membership certificate or ALTA Policy Forms License is received the Company President will maintain it in a secure file in their office.

4. This procedure will be repeated each year prior to the expiration date of the current ALTA membership certificate, ALTA Policy Forms License or Occasional Use Waiver.

BEST PRACTICE TWO (2) – ESCROW ACCOUNT CONTROLS

Definition: ***Adopt and maintain appropriate written procedures and controls for Escrow Trust Accounts allowing for the electronic verification of reconciliation.***

Shield Title AZ Policy and Procedures: All escrow funds are maintained in separate designated accounts which are reviewed for reconciliation discrepancies on a daily basis. These accounts are monitored under the following controls:

- Daily reconciliation of all debts and credits to the account as well as available balances using the latest version of AccuTitle/ Title Desktop settlement software and Rynoh Reconciliation Software.
- Positive Pay and ACH Debt blocks setup on all accounts.

- Open escrow balances and outstanding checks are reviewed by management on a weekly basis.
- Three Way Reconciliations completed on a monthly basis and reviewed for accuracy by management.
- Appropriate authorization levels are set and maintained.

2.1 - ESCROW/ TRUST ACCOUNT CONTROLS

Shield Title AZ ("the Company") has internal controls in place that apply to all custodial and fiduciary accounts ("Trust Accounts") to meet client and legal requirements for the safeguarding of client funds and to minimize the exposure to loss of client funds.

ESCROW CONTROL PROCEDURES

The Company has one active Trust Account that is established and maintained in accordance with state regulations and its agency underwriter contract. All client funds collected as a fiduciary are deposited into these accounts. The Trust Account is maintained separate from all other Company accounts, including operating and personal accounts. The Company President maintains a log of all bank accounts in the Company's name.

The Trust Accounts are maintained at Comerica Bank, a financial institution whose deposits are insured by the FDIC. The accounts are titled and clearly identified as "Shield Title AZ Trust Account" on all bank statements, bank agreements, disbursement checks and deposit tickets. This is to confirm the fiduciary nature of the account.

DAILY PROCEDURES AND CONTROLS

1. All funds collected from parties at settlement are deposited into the Trust Account. Collected funds may be in the form of a wire, cashier's check (for anything over $500) or personal check (for anything under $500).

2. All checks received at settlement are restrictively endorsed "For Deposit Only" upon receipt. A separate deposit ticket with corresponding file number is prepared for each file and the deposit is made within twenty-four hours of receipt.

3. Funds are only disbursed after the collected funds have been deposited into the Trust Account and irreversibly credited to it.

4. Incoming and outgoing wire confirmations are maintained in each file.

5. Each check written out of the Trust Account must reference the corresponding file number that it was written for. Copies of the checks are maintained in the file along with a current, detailed deposit and disbursement summary sheet.

6. All check stock is safeguarded in a secure, locked location that only authorized check signers can access. All check stock is accounted for by the Company President at the end of each business day.

7. Any instructions that the Company receives for specific handling of escrow funds from a particular party must be made in writing and kept in the transaction file. If a separate, interest-bearing account is requested same will be established and be subject to the same procedures outlined here.

8. Inactive or dormant account disbursements must be approved by the Company President. This approval must be in writing and be maintained with the account's bank statements and reconciliations.

9. Disbursements from any file that is more than 180 days old must be approved by the Company President. This approval must be in writing and be maintained in the file.

MONTHLY PROCEDURES AND CONTROLS

All bank fees including service charges and wire fees are reimbursed with funds from the Company's operating account.

2.2 - ESCROW/ TRUST ACCOUNT AUTHORIZATIONS

Shield Title AZ ("the Company") has internal controls in place to ensure that only employees that have passed background checks are authorized to sign checks, initiate wires, and approve bank account transactions for all custodial and fiduciary accounts ("Trust Accounts") and further that all Trust Account transactions are initiated or approved only by such authorized employees.

Currently, Omar Qader (President/Owner) is the only authorized signatory with access to our Escrow Account, sign checks and initiate wires.

TRUST ACCOUNT AUTHORIZATION PROCEDURES

1. At the beginning of each calendar year, the Company President/Owner considers if any additional employees should be authorized to approve financial transactions, sign checks and initiate wires for the Company's Trust Account. At the same time the Company President considers limits for each employee that would be authorized.

2. Should additional employees be authorized, the Company President would create a Trust Account Authorizations Log to be maintained for the entire calendar year with any authorized employees' names, respective authorizations and limits.

3. All employees authorized to process Trust Account transactions must undergo and pass a background check at the time of hiring and/or prior to being authorized. The background check will include criminal and consumer credit reports that cover a period of not less than five (5) years. Established employees with Trust Account authorizations will undergo a background check at least every three (3) years. The results of the background checks will be maintained in a secure personnel file in the President's office.

4. When an authorized employee leaves the Company or when the Company President decides to cancel an employee's authority, all of their Trust Account authority is canceled immediately; any necessary bank paperwork is completed immediately and the Trust Account Authorizations Log is updated.

5. The Company has the following controls in place to ensure that Trust Account bank transactions are conducted by authorized employees only:

- The Company does not permit the use of signature stamps on Trust Account checks
- All checks require the "wet" signature of the Company President/Owner
- All outgoing wires require dual authorizations with password (key fob) verification
- All check stock is maintained in a locked cabinet that only authorized employees have access to.

7. Per the Company's instructions, the bank has a block on the Trust Account for Automated Clearing House (ACH) Transactions.

8. Per the Company's instructions, the bank has a block on the Trust Account for International Wire Transactions.

9. The Trust Account is set-up with Positive Pay so that the bank only clears checks after verifying them with the Company's check register.

2.3 – TRUST ACCOUNT RECONCILATION PROCEDURES

Shield Title AZ ("the Company") shall have procedures and controls in place to ensure Three-Way Reconciliations are performed on all custodial and fiduciary accounts ("Trust Accounts") monthly basis; that same are reviewed and signed off by management and that appropriate follow-up is performed on outstanding and trial balance items.

DAILY PROCEDURES AND CONTROLS

1. When the Company conducts a settlement, all funds collected are deposited into the Company's Trust Account.

2. Funds are only disbursed by an authorized employee after they have verified that the collected funds have been deposited and irreversibly credited to the Account and that the collected funds are sufficient to cover the disbursements.

3. A separate receipt and disbursement ledger is printed and maintained in each settlement file detailing every receipt and disbursement including date, amount, payee/payer and description.

4. The ledger should indicate that the file balances (Receipts = Disbursements) or there should be documentation to support any difference (i.e. – escrow agreement for funds being held).

5. The Company President or their designee performs a daily reconciliation through Rynoh of all Trust Account receipts and disbursements.

MONTHLY PROCEDURES AND CONTROLS

1. The Trust Account bank statement is delivered to and opened by the outside CPA who is responsible for performing a Three-Way Reconciliation of the Account. The outside CPA is not an authorized signer or wire initiator on any of the Company's bank accounts.

2. Within ten (10) days of receiving the bank statement, the outside CPA completes a Three-Way Reconciliation of the account in accordance with approved Three-Way Reconciliation Procedures.

3. Deposits in transit and outstanding checks on the previous month's Three-Way Reconciliation are checked against the current bank statement to determine what has cleared and what remains outstanding.

4. Upon completion of the Three-Way Reconciliation, the outside CPA prints the following reports:

- Summary page with Register/Book Balance, Trial Balance, Adjusted/Reconciled Bank Balance
- Cleared Transactions/Proofing Register
- Deposits in Transit
- Outstanding Checks
- Trial Balance (Unbalanced Files
- Reconciling items
- Voided Checks
- Outstanding checks from previous month

5. Within one day of completion of the Three-Way Reconciliation Reports the outside CPA provides them to the Company President who reviews them for completeness and accuracy. The Company President Initials and dates the front page to document their review.

6. The Company President, outside CPA and staff work together to immediately research and resolve any of the following items reflected by the Reconciliation Reports:

- Deposits in Transit older than five (5) days

- Incoming Wires in Transit older than two (2) days
- Payoff and Proceeds checks outstanding for more than ten (10) days
- Recording checks outstanding for more than thirty (30) days
- Checks for taxes and/or hazard insurance outstanding for more than thirty (30) days
- Underwriter premium checks outstanding for more than sixty (60) days
- All other checks outstanding for more than ninety (90) days
- Reconciling items

Documentation of all resolved items is maintained with the statement and reconciliation reports.

7. Any escrow shortages are immediately funded from the operating account.

8. All bank fees are reimbursed on a monthly basis from the operating account.

9. Copies of the bank statement and Three-Way Reconciliation Reports are made available electronically to the Company's title insurance underwriter.

10. The Company President periodically reviews cancelled checks and the check register for unusual items.

ANNUAL PROCEDURES

Each year the Company President and outside CPA review the outstanding checks and file ledger balances for reissue or escheatment to the State as required by law.

BEST PRACTICE THREE (3) – INFORMATION AND DATA PRIVACY

Definition: ***Establish and maintain a written privacy and information security program to protect Non-Public Personal information as required by local, state and federal law.***

Shield Title AZ Policy and Procedures: Shield Title AZ has a comprehensive security program designed to insure that all necessary information security safeguards are in place and adequately address GLBA requirements. All employees of the Company are expected to contribute to this program and report any incidents that may affect the security of the organization's information systems. The following policies are addressed within Shield Title AZ's Information Security Policy.

- Controlled access to physical and electronic storage as well as secure destruction of physical documents
- Secure transmission of information
- Monitoring of third party service providers access
- Physical entry controls to prevent unauthorized access

- Network guidelines and access controls including restrictions on user authentications and authorization
- Remote access controls and restrictions
- Up to date virus management software and firewall controls against malicious software, viruses and unauthorized websites
- Business Continuity Plan for disaster preparedness
- Security Incident Reporting and Resolution
- Background checks on all personnel
- Training of employees to ensure compliance with program
- Restrictions and the appropriate uses of company systems

3.1 – Information Security and Privacy Management Procedures

Shield Title AZ ("the Company") is committed to protecting non-public, personal, and/or sensitive information ("Private Information") as required by local, state, and federal law. The Information Security and Privacy Management Policies outlined herein have been adopted by the Company to ensure compliance with the applicable laws and to ensure Private Information is properly safeguarded.

The Company has created and adopted written procedures and an Information Security Program to ensure that it is compliant with federal, state, and local laws and able to best protect its clients' confidential, personal, and/or Private Information. This written **Information Security Program** is outlined in procedure reference no. 3.4 herein. It specifically addresses protection of non-public Private Information and provides direction for managing and protecting the confidentiality, integrity and availability of all of the Company's information assets. Following are additional components of the Company's Information Security and Privacy Management policies.

1. Background Checks / Hiring Practices – The Company seeks out and hires only qualified employees with verified education credentials, work history and reputations. The Company performs background checks, including criminal history, on employees and temporary staff that have access to Personal Information. Such employees will have a background check at least every three (3) years. The results of background checks are maintained in the employee's personnel file as per the Company's document retention and destruction guidelines.

2. Acceptable Use of Information Technology Policy - The Company's Acceptable Use of Information Technology Policy is outlined in procedure reference no. 3.4.1 herein describing the ways and circumstances under which employees may use Company owned technology.

3. Access to Private Information - Private Information held by the Company is restricted to only those employees whose job duties require access to this information. Access to Private Information is granted and authorized by the Company's President. These access rights are reviewed annually to ensure the correct permissions are granted to the Company's employees.

4. Clean Desk and Clear Screen Policy - The Company has a Clean Desk and Clear Screen Policy that is further outlined in procedure reference no. 3.4.2 herein.

5. Data Security- Removable Media - The Company has a removable media policy outlined in procedure reference no. 3.4.3 herein that restricts the use of USB devices, CD/DVD writeable drives and other storage devices.

6. Record Retention and Disposal Policy - The Company has a Record Retention and Disposal Policy that is further outlined in procedure reference no. 3.5 herein.

7. Approval - The Company's Information Security and Privacy Management has been approved by the Company President. It is communicated to all employees annually by the office manager and all employees are required to sign an acknowledgment of their receipt. The acknowledgment is retained in each respective employee's personnel file. The Company ensures that all employees are aware of their individual roles in the protection of Private Information by routine staff meetings, training session and continuing education seminar presented by our underwriters.

Limited exceptions to any of the Company's policies may be approved by the Company President. Exceptions to policies are documented in a designated file and retained as per the Company's document retention and destruction guidelines. Employees who violate any of the Company's policies are subject to disciplinary action up to, and including termination.

8. Policy Review - The Company's Information Security and Privacy Management Policies are reviewed as further outlined in the Company's Policy Review Procedures Policy (procedure reference no. 3.1.1 herein) to determine if updates are necessary to reflect changes in operations, legal and regulatory requirements, industry best practices and available technology. Changes to any of the Company's policies are tracked and maintained as further described in that Policy Review Procedures Policy.

9. Customer Privacy Notice - The Company has a Customer Privacy Policy Notice, which is provided to customers with the delivery of the title commitment by email. The customer must initial or sign the Notice to acknowledge their receipt it and the initialed or signed copy is retained in the Company's transaction file.

10. Privacy Statement - The Company's website contains a Privacy Statement, which includes details regarding information, if any, that may be collected.

3.1.1 – IS Policy Review Procedures
Shield Title AZ ("the Company") reviews and updates all Information Security and Privacy Management Policies on a regularly scheduled basis to determine if updates are necessary to reflect necessary to reflect changes in operations, legal and regulatory requirements, industry best practices and available technology.

1. Review Team - The Policy Review Team will**,** on an annual basis and more frequently when required, meet to review all Information Security and Privacy Management Policies. The Policy Review Team will consist of the Company President and Shivan Amani, our outside IT Consultant. Changes to the policies are only made after these meetings.

2. Review Criteria - A variety of criteria will be used by the Policy Review Team at the time of review. These items will include reviewing the policy to determine if changes to any of the following have been made:

- Company operations;
- Legal and Regulatory requirements;
- Industry Best Practices;
- Available Technology

3. Communication - Upon completion of the review and necessary revisions to any Company policies, updated policy versions will be placed in the company's official policy manual, replacing the outdated version. The updated policies will be communicated to all staff members, as well as any clients, when appropriate. All staff members are required to review and acknowledge receipt of the new policy manual via the company's policy acknowledgment form. Said acknowledgment will be retained in the employee's personnel file.

3.2 – Risk Identification and Assessment Procedures
Shield Title AZ ("the Company") is committed to protecting non-public, personal, and/or sensitive information ("Private Information") as required by local, state, and federal law through its Information Security and Privacy Management policies. Operations are regularly reviewed to identify and assess current or suspected external and internal risks that could compromise the Private Information stored by the Company.

The Company has created and adopted written policies and procedures with the goal of identifying and assessing current or potential risks which could have a negative effect on the Company, its systems, or clients, including risks that could compromise Private Information held by the Company. Private Information is defined under this policy as any privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the Company. These procedures include the regular review by Policy Review Team of the Company's operational functions to identify potential or actual risks.

This review will include examination of:

- The types of Private Information the Company maintains;
- The location in which Private Information is stored;
- How information can be accessed;
- Which employees have access to Private Information;
- Which non-employees have access to the office

Risk Assessments performed by Policy Review Team includes internal and external risks. The risk analysis review encompasses the Company's entire computer networking system(s) and physical security tools including but not limited to alarm system, entrance and interior door locking mechanisms (key pad) and locks on file cabinets.

All employees play a major role in the identification and elimination of risks to the Company. Employees receive training on ways they can help identify risks and ways to avoid compromising the Private Information for which they have access. Employees of the Company may create unintended risk while performing normal business functions for the Company. The Company takes steps to limit the risk created by employees which may include:

- Limiting the amount of information each employee may access to only that information needed to perform the duties associated with the employee's position;
- Reviewing how information is communicated to clients, lenders, vendors, and all other third parties involved in the transaction to ensure that transmission is safe, encrypted, and otherwise protected during transit;
- Identifying ways information is and may be protected when it is accessed outside of the Company's office(s) by Company employees, including mobile devices, laptops, etc.

The Company President is responsible for authorizing each employee's access to Private Information. The Company has controls in place to prevent improper access of Private Information by all employees who have not been granted the appropriate security permissions. These controls are regularly tested by the Company President or their designee.

The Company's President documents the risk analysis results and records changes made to the Company's information security network or operations to eliminate or reduce risk for the Company. This documentation, including all change management records, is retained in a designated file as per the Company's document retention and destruction guidelines.

3.3 – Employee Training, Management and Responsibilities Procedures

Shield Title AZ ("the Company") is committed to protecting non-public, personal and/or sensitive information ("Private Information") as required by local, state, and federal law through its Information Security and Privacy Management policies. All Company employees are

trained on the Company's Information Security and Privacy Management policies to ensure they fully understand the importance of adherence to the Company's policies and the protection of Private Information.

All Company employees have the responsibility to understand how to protect confidentiality, integrity, and availability of information systems. Awareness training improves the user's awareness of the company's Information Security policies and procedures and the need to protect information resources. Training makes the system users aware of their role in protecting information, their security responsibilities, defines the user's role in the security process and helps the user develop skills and knowledge so that they may perform their jobs securely.

New employee training: All employees hired by the Company or individuals employed on a temporary basis will undergo specific training programs relating to the Company's Information Security Program including the following subjects:

- Security Awareness;
- Risk Analysis;
- Privacy Issues;
- Clean Desk and Clear Screen Policy (procedure reference no. 3.4.1 herein)
- Identification of Private Information;
- Responsibilities every employee has to protect Private Information including controls and procedures to prevent Private Information disclosure to unauthorized parties;
- Consequences for non-compliance;
- Acceptable use of the Company's computer system, network, equipment, and devices;
- Proper use of computer networks and passwords;
- Methods for proper disposal of documents containing Private Information

New employees are given copies of all of the Company's policies and procedures relating to Information Security, Protection of Private Information and Acceptable Use of Information Technology on the first day of employment with the Company. An acknowledgment of receipt and comprehension of these procedures will be executed by the employee and maintained by the Company President or their designee.

All employees of the Company will be provided with updates to these policies immediately after the updates are made to these policies and procedures. Employees will receive training, at least annually, on the Company's information security policies and procedures and will complete a training acknowledgment form every time an updated training session is completed. An Information Security Training Log is maintained by the Company President or their designee. Training that is performed at least annually and training of new employees will include the following items related to the information security policies:

- Security Awareness;
- Risk Analysis;

- Privacy Issues;
- Clean Desk and Clear Screen Policy (procedure reference no. 3.3.1 herein)
- Identification of Private Information;
- Protecting Private Information including controls and procedures to prevent Private Information disclosure to unauthorized parties;
- Consequences for non-compliance;
- Acceptable use of the Company's computer system, network, equipment, and devices;
- Proper use of computer networks and passwords;
- Methods for proper disposal of documents containing Private Information

3.4 – Information Security Procedures

Shield Title AZ ("the Company") is committed to protecting non-public, personal, and/or sensitive information ("Private Information") as required by local, state, and federal law. The Information Security Policy outlined herein has been adopted to ensure compliance with the applicable laws and to ensure Private Information is secure. The Company's Information Security Policy provides direction for managing and protecting the confidentiality, integrity and availability of all of the Company's information assets, including the Company's network, systems, equipment and other devices. The Company has several policies in place, including but not limited to the ones outlined herein to protect against unauthorized access to physical files and systems the Company uses to store or process Private Information is properly safeguarded.

1. Statement of Responsibility - The Company President is responsible for the administration of this policy and responsible for maintaining procedures; user access, updating systems and documentation; providing appropriate support and guidance; reviewing the policy annually; Company employees are responsible for adhering to the policies and procedures for notifying the Company President of any issues or violations.

2. Violations - Employees found to be in violation of this policy are subject to disciplinary action that is commensurate with the severity of the violation.

3. User Access – The Office Manager and Company President determine the level of access for each employee of the Company and coordinate same with the staff of Shivan Amani. Access is limited to only employees that need access to carry out their daily job functions. Access privileges are reviewed annually by the Company President. Access privileges are adjusted immediately anytime an employee is terminated or changes job functions and anytime contractor or third-party severs its relationship with the Company.

4. User IDs and Passwords – Unique user IDs and passwords are issued to all employees accessing the Company's systems. Each employee must safeguard their User ID and Password from all other persons including other employees. Compromised passwords must be reported immediately to the Company President. Systems are configured to record the user ID used to

access them. Passwords must be at least seven (7) characters long and contain at least one Capital letter, one number and one special character. Monitors lock after five (5) minutes of inactivity requiring a password to unlock. Passwords must be changed every 60 days. After five (5) invalid login attempts the user ID will be suspended. It can only be re-activated by System Administrator.

5. Acceptable Use of Information Technology – See procedure reference no. 3.4.1 herein

6. Data Security – See Clean Desk and Clear Screen Policy (procedure reference no. 3.4.2) herein and **Data Security – Removable Media Policy** (procedure reference no. 3.4.3) herein

7. Data Backup – Servers are backed up daily via Epic Software through their cloud based settlement software website in accordance with the terms of our agreement.

8. Physical Security - The Company limits access to its office to only those individuals who require access for legitimate business functions. Access to the office is limited including unique locks, key pad access, restricted access and alarm system. Restricted areas are marked by signage restricting access to authorized personnel only. If an employee with access rights is terminated or otherwise leaves employment of the Company, the Company President retrieves all office keys and terminates all access and passwords through administrative rites.

9. Electronic Security - Security Controls are in place to prevent unauthorized access, misuse, or corruption of Private Information by secure Windows Defender firewall tools with detection and prevention features, complex password protocols, Microsoft Security Essentials anti-virus software and secure Windows Defender email transmission. These controls are in place for the data- base/network access and email systems. These controls are in place for information during the electronic transmission of the data as well as when the information is held in storage.

10. Equipment - Employees may be granted use of the Company's equipment, including items such as laptops, smartphones containing the Company's email or other network information. The Company prohibits the use personal equipment to access the Company's data. All employees who have the authority to use equipment belonging to the Company off-site must immediately report loss or theft of these items to the Company President.
All equipment, hardware and software assigned to employees, contractors or other third-parties must be returned immediately upon their separation or termination from the Company.

11. Network Security Controls -

Firewall Protection - The Company uses firewalls to protect all network entry points The Company utilizes Windows Defender Firewall tools that include network intrusion detection and prevention features to protect the network. Our network is continuously monitored by Windows Defender who receives and re-acts to any alerts or intrusions detected.

Anti-Virus Protection - The Company uses Anti-virus Software to protect the Company's network systems (servers, workstations and laptops) and data against malicious threats. The Company utilizes Microsoft Security Essentials Anti-virus software to prevent, detect and eradicate threats to the network. Scans are set to run nightly with updates pushed automatically. Microsoft Security Essentials is installed for protection at the server level as well as individual workstations.

12. Remote user access ("Remote Access") – Remote Access to the Company's network and or data is strictly prohibited by employees. The Company President must approval any exceptions to this policy.

13. Wireless Devices – The Company strictly prohibits the use of Wireless Devices to access the network/database. The Company does not allow any personal devices such as laptops, computers mobile devices, smartphones, etc. to connect to our wireless network via the wireless technology or wired technology. Unless provided by the firm, no devices are allowed to connect to the enterprise network.

14. Separation of Duties – Windows Defender (outside IT Consultant) is not authorized to perform transactions within any of the Company's systems that contain Private Information.

15. System Modifications - The Windows Defender (our IT Consultant) is responsible for performing regular updates to install patches and other software updates/fixes designed to keep systems current and to mitigate known security flaws. New or updated technology, including hardware or software, is tested before it is implemented. Updates made to software or hardware is documented and maintained by the Company President.

16. Additional Measures

The Company has the following additional policies in place to protect against additional information security concern:

- Risk Analysis and vulnerability testing;
- Access logging

3.4.1 – Acceptable Use of Information Technology Procedures

Shield Title AZ ("the Company") has the following Acceptable Use of Information Technology Policy to ensure that the use of the Company's electronic based communication systems and business equipment including e-mail, voice mail, and internet access and accounting systems is consistent with the business interests of the Company and in the interest of its clients.

1. **Communications -** All communications are the property of the company. They are business records and may have legal and operational effects identical to those of traditional hard copy documents. Accordingly, all electronic communications should be treated as though they may later be viewed by others. Employees should have no

expectation that any information transmitted over company facilities or stored on company computers is or will remain private.

The company may access, monitor, disclose or distribute any communication associated with any electronic equipment or system employed by the company. It is also possible that non-employees may gain access to company communications through on-line services or specific access to our hardware or systems. For these reasons, it is very important to use good judgment in creating, distributing and retaining e-mail, voice mail, internet/intranet or other electronic documents and messages.

Password protection is required for any of your network communications, and employees must follow all protocols and procedures. Never disclose your password to anyone unless that person has the proper clearance and a legitimate need to know. The Company President or their designee may authorize use of an employee's password during temporary absences for illness or vacations. Passwords must be changed upon the employee's return to work.

2. Conditions of Use of the Information Technology System

Definition: The term **Information Technology System** is used as a synonym for computers and computer networks used to store, retrieve, transmit, or manipulate data, but it also encompasses other information distribution technologies such as television and telephones.

The Information Technology Systems are the property of the company, and users should understand that any use of these systems is not private or confidential.

2.1. Prohibited Use of Information Technology Systems - Transmitting, storing or accessing obscene, vulgar, profane, insulting or offensive material or messages (such as ethnic slurs or sexually explicit words, photographs and/or drawings) or other material that could be construed as disparaging to any person based upon that person's sex, race, age, national origin, disability or religion.

Receiving, printing, transmitting, or otherwise disseminating proprietary data, client information, PII (personal identifiable information) company secrets, or other confidential information in violation of company policy or proprietary agreements is strictly prohibited. Downloading inappropriate material such as picture files, music files, or video files for personal use is also strictly prohibited.

The Company strictly prohibits the use of all Company equipment (internet, phone and email system) for personal use. The Company permits the use of personal cell or smartphones during breaks and lunch time.

3. Monitoring Usage of Information Technology Systems - The Company may, from time to time at its sole discretion, monitor use of the Information Technology Systems. Such monitoring

may include the interception of telephonic communication and voicemail messages, printing and reading data files (including personal documents, E-mail, messages and attachments) and monitoring internet usage (including a review of time spent on the internet and a review of specific web sites visited).

4. Restricted Internet Traffic - The Company's Internet system is restricted and intended only for business purposes. The Company strictly prohibits the use of the Company internet system by employees for personal use. Employees are permitted to access the internet through personal smartphones or tablets during breaks and lunchtime. Our Windows Defender firewall restricts access to questionable sites and content.

5. Blogging Policy – The Company prohibits employees from blogging in the Company's name. The above policy applies to all other forms of social networking media or technology on the Internet, radio, television or in print media. It is the company's right to protect itself from unauthorized disclosure of information or distribution of information or opinions that are detrimental to the company.

6.0 Software Code of Ethics - Unauthorized duplication of copyrighted computer software violates the law and is contrary to our company's standards of conduct. We disapprove of such copying and recognize the following principles as a basis for preventing its occurrences:

- The making or using of unauthorized software copies is not permitted under any circumstances.
- Legally acquired or purchased software required by the company will be provided to meet the legitimate software needs in sufficient quantities for company computers.

8.0 Violations - Employees who violate this policy are subject to disciplinary action including training, probation and termination.

3.4.2 - Clean Desk and Clear Screen Policy

Shield Title AZ ("the Company") is committed to protecting non-public, personal and/or sensitive information ("Private Information") as required by local, state, and federal law through its Information Security and Privacy Management policies. All employees are responsible for following the Clean Desk and Clear Screen Policy outlined herein to reduce the threat of a security breach, fraud and information theft of electronic and physical documents located on the Company's premises.

1. Purpose - This policy will establish a culture of security and trust for all employees and clients by ensuring the company is taking the appropriate responsibility for the Private Information in its care. It reduces the risk of unauthorized access to, loss of, or damage to information, thereby reducing the chance of breach of client confidentiality and theft of intellectual property. Additionally, a clean desk will provide a professional and positive image to office visitors, including clients, by ensuring an appropriate office appearance while meeting health and safety considerations.

2. Responsibilities - The Company President is responsible for implementation and enforcement of this policy. All employees must comply with the terms of this policy as they pertain to their specific job responsibilities.

3. General Requirements - Each employee must:

- Lock, with Password Protection, the computer system every time a workstation is left unattended for any period of time.

- Set the computer's automatic locking feature to lock, with Password Protection, the idle computer after 15 minutes of system inactivity.

- Log off the computer system at the end of each work day.

- Remove all files, documents, and/or Information Technology (IT) devices containing Confidential Information, as further defined in the Company Information Security Policy, from the work space and lock these items in a drawer when the workstation is left unattended or at the end of the work day. The key for the locked drawer is to remain with the employee at all times and may not be left unattended. A second key for the locked drawer will remain with the Company President and may not be left unattended.

- Lock file cabinets or drawers containing Confidential Information when not in use.

- Keep the workstation and any other accessible areas clear from Sensitive Information. Sensitive Information is any privileged or proprietary information which, if compromised, could cause serious harm to the Company. This Sensitive Information may include, but is not limited to, user ids, passwords, and account numbers. This Sensitive Information is maintained and kept secure in the employee's locked desk and with a copy maintained in the Company President's secure file cabinet.

- Immediately remove printed documents that may contain Confidential Information from printers, copiers and/or facsimile machines and place these items into the appropriate secured physical file. These items may be temporarily secured in the employee's locked drawer referenced above until the time when said file is actively being processed, but must be put into the appropriate file before the end of the business day.

- Shred any document containing Confidential Information as soon as the document is no longer needed via our shredding vendor or the company shredding machine located in the office.

4. Enforcement - Employees are expected to follow the spirit and intent of this policy. Periodic sweeps of work areas may be conducted by the Company President or a designee to verify

adherence to this policy. Violations of this policy may result in disciplinary actions, up to and including termination.

5. Revisions - This policy will be reviewed on an annual basis and appropriate changes will be made accordingly.

3.4.3 – Data Security- Removable Media

Shield Title AZ ("the Company") is committed to protecting non-public, personal and/or sensitive information ("Private Information") as required by local, state, and federal law through its Information Security and Privacy Management policies. All employees are responsible for following the Data Security Policy outlined herein to minimize the risk of loss or exposure of sensitive data maintained by the Company and to reduce the risk of acquiring malware infections on Company computers.

1. The Company prohibits the use of any removable media (i.e. – CDs, DVDs, Flash/Thumb drives) for the purpose of making a copy of Company data. Exceptions may be granted by President. Any such exceptions must be documented. Any removable media devise should be encrypted to prevent access by unauthorized parties.

2. CDs and Flash/Thumb drives should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they should be locked in a secure location.

3. CDs and Flash/Thumb drives should be kept away from environmental hazards such as heat, direct sunlight and magnetic fields.

4. Critical computer equipment is protected by uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.

5. Environmental hazards to hardware (i.e. – food, liquids, smoke, high or low humidity and extreme heat or cold) should be avoided.

3.4.4 - Information Sensitivity Policy

Shield Title AZ ("the Company") is committed to protecting non-public, personal, and/or sensitive information ("Private Information") as required by local, state, and federal law. The Information Sensitivity Policy outlined herein has been adopted to ensure employees understand what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the Company without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means, including: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect the Company Private Information, as defined below, (e.g., Confidential Information should not be left unattended in conference rooms).

Scope. All information is categorized into two main classifications:

- "Public Information" contains all information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the systems.

- "Confidential Information" contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Confidential Information also includes information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

- A subset of Confidential Information is "Third Party Private Information". This is Private Information belonging or pertaining to another corporation or individual which has been entrusted to the company by that third party under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive information to information about the fact that we have connected a supplier / vendor into a network to support our operations.

Company employees are encouraged to use common sense judgment in securing Confidential Information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, then the employee should contact the appropriate manager.

Sensitivity: Generally - The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these Sensitivity Guidelines as a reference only, as Confidential Information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of information in question.

- **Minimal Sensitivity:** General corporate information; some personnel and technical information. This information is to be designated and always treated as "Confidential". All employees approved to view and access Non-Public Information may have access to and process this information. This information may be sent outside the office by U.S. Mail, encrypted email or overnight courier.

- **More Sensitive:** Business, financial, technical, and most personnel information. This type information is to be designated and treated as “Sensitive Confidential”. Access to and the processing of this information is restricted to employees assigned to process the file or task. This information may be sent outside the office to authorized recipients by encrypted email or overnight courier with a unique tracking number. This information should be destroyed/shredded at the earliest point when it is no longer needed. Violators will be subject to discipline including termination.

- **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company is to be designated and treated as “most sensitive confidential”. Access to and the processing of this information is only authorized by the Company President. This information may only be sent outside the office by the Company President or his approved designee. Violations to this section, whether deliberate or inadvertent, are subject to termination. Retention and destruction of this information is at the sole discretion and direction of the Company President.

Information Sensitivity and Computer Usage - To minimize risk to the company from an outside business connection: Computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access corporate information, the amount of information at risk is minimized. The Company utilizes secure Windows Defender firewall tools with detection and prevention features, complex password protocols, Microsoft Security

Windows Defender software, redundant network backup procedures and secure Windows Defender email system.

Information Sensitivity and company-to-Other Business Connections - Connections, such as third-party service providers, must be set up to minimize the information available to other businesses. The company ensures that these third-party providers see only the information necessary to complete the contracted services.

Delivery of Sensitive Information - Sensitive information should always be delivered in person or by secure email.

Enforcement - Any employee found to have violated this policy may be subject to disciplinary action including training, probation and termination.

3.5 – Retention & Destruction of Private Information

Shield Title AZ (“the Company”) is committed to protecting non-public, personal, private and/or sensitive information (“Private Information”) as required by local, state, and federal law through its Information Security Program. The retention and destruction of Private Information in the Company’s care will be handled in accordance with the procedures outlined herein which have been derived in compliance with applicable law and contractual requirements.

The Company has created this Retention and Destruction of Private Information Procedure for all official documents containing, or suspected to contain, Private Information. All Company employees and contractors are informed of their responsibilities regarding the handling, protection and destruction of Private Information prior to being assigned any job duties that involve handling of same.

Definition of Private/Non-public Information for the purposes herein - Personally identifiable data such as information provided by a customer on a form or application, information about a customer's transactions, or any other information about a customer which is otherwise unavailable to the general public. Private information includes 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 number(s).

How Private Information is Obtained - Documents with Private Information are obtained by the Company within the course of its normal business operations. These procedures were created in accordance with the requirements of all applicable laws and contractual obligations to ensure that official records no longer needed are discarded at the appropriate time. The procedures provide guidelines concerning the length of time official records should be retained under ordinary business circumstances.

Retention and Destruction - When documents that may contain non-public personal information are determined to be no longer needed for the transaction or service for which it was provided will be destroyed by the company shredding machine.

Hard drives located in the Company's equipment, including computers and copiers are removed and physically destroyed before equipment is disposed or reused. Hard drives located in equipment that has been leased by the Company are removed and physically destroyed prior to being returned. All other information technology media including stand-alone hard drives, tapes, flash drives, or other types of removable media include physically destroying hard drives or scratching the surfaces and breaking into pieces for media such as disks and CD-ROMs. Inactive documents containing financial information, which may include account information, are retained indefinitely but always for a period of not less than seven (7) years.

Inactive documents containing personal information, which may include personnel records, are retained for a period of not less than seven (7) years. This type information is retained in locked file cabinets in the Company President's office until destruction is to occur.

Old transaction files, or documents pertaining to those files, are retained for a period of not less than ten (10) years. Upon full completion of the file, paper files are scanned into Epic Software and transfer to off-site storage with restricted access, security system and unique locks. After the retention period, paper copies of transactional files are shredded. The Company President oversees this process and reviews this information annually for destruction.

After this retention period, old transaction files will be reviewed annually by the Company President for eligibility for destruction. Eligible file will be shredded.

3.6 – Overseeing Service Providers Policy

Shield Title AZ ("the Company") is committed to protecting non-public, personal, private, and/or sensitive information ("Private Information") as required by local, state, and federal law through its Information Security Program and written procedures. Any third-party service providers used by the Company that require access to Private Information will be subject to the oversight procedures outlined herein.

Third party service providers utilized by the Company to assist with operation or other business functions, and/or to provide services for real estate transactions may require access to non-public personal information in order to perform the services they provide. These vendors may include but are not limited to:

- Title Examiners;
- Surveyors;
- Shredding/Destruction Services;
- Credit Reporting Services;
- Information Technology Vulnerability Testing Companies
- Title Insurance Underwriters (Auditors and Agency Representatives)

The Company performs reasonable, due diligence checks on all vendors prior to use, which may include:

- background checks and/or reference checks;
- review of information policies and procedures, financial resources and references;
- review of outside audits or Statement on Standards for Attestation Engagements (SSAE- 16)
;

The Company prefers to use known industry leaders for services provided. Vendors are required to maintain errors and omission coverage which, at a minimum, meet any state, industry, and contractually obligated requirements.

All third-party service providers are required to execute a Confidentiality Agreement addressing the security and protection of Private Information before any services are provided and before access to potential Private Information is granted.

All third-party vendors are required to maintain, at a minimum, the same information security procedures as the Company. The procedures include requirements for the vendor to maintain a written Information Security Program. The vendor's program may include policies for:

- Physical and Electronic Security;
- Acceptable Use Policies;

- Password Policy;
- Business Continuity and Disaster Recovery Policies;
- Risk Analysis;
- Retention and Destruction;
- Security Awareness;
- Change Management

The Company President is responsible for managing all vendor relationships. These responsibilities include oversight of each vendor and ensuring that all of the vendor's insurance coverage declaration records maintained by the Company are kept up to date. This type information is retained in a designated file in the Company President's office. The Company President or their designee monitors the vendor's service level, pricing, and contractual obligations to ensure that the vendor is performing services securely, accurately, and professionally. Vendors are contractually obligated to the Company to remedy privacy or other performance requirements; other-wise they risk termination of services.

3.7- Data Breach Incident Reporting Policy

Shield Title AZ ("the Company") is committed to protecting non-public, personal, private or sensitive information ("Private Information") as required by local, state, and federal law through its Information Security Program and written procedures. Any data breaches or other information security incidents (intentional or unintentional) will be handled in accordance with the procedures outlined herein.

The Company has tools in place to limit its exposure to incidents involving data breaches or other inappropriate access to sensitive information including Windows Defender Firewall tools that log any intrusion attempts and provides an IP address including a timestamp, Microsoft Security Essentials anti-virus software for virus detection and prevention and SSL encryption prevents personal information from being transmitted in clear test avoid security incidents. The Company monitors external threats (attacks/intrusions) to its information network and systems by continuous monitoring by Windows Defender, our outside IT Consultant.

All employees are required to attend training regarding incident response as part of their Information Security Program training. This training includes information on how actual and suspected data-breach incidents are to be reported, investigated, and handled. Employees receive copies of all written policies and procedures relating to incident response as part of this training program.

When a potential attack or intrusion is discovered, Windows Defender receives notifications and responds according to the level of threat detected. Include who receives report of the attack internally. The staff of Windows Defender is responsible for collecting data for the incident response including audit trails and access logs. Investigations of incidents are handled by Windows Defender and when appropriate, escalates information relating to these attacks

the Company President to determine whether the incident must be officially reported per federal, state, and local laws and/or contractual agreements.

Employees found in violation of any of the Company's information security policies will be subject to disciplinary action up to, and including, termination.

3.8 – Business Continuity & Disaster Recovery Plan

Shield Title AZ ('the Company") has adopted the Business Continuity and Disaster Recovery procedures outlined herein as part of the Company's Information Security Program. These procedures are in place to assist the Company in a timely resumption of business activities should it experience an unexpected information system failure, including emergency or disaster situations.

The Company's Disaster Recovery Plan provides written instructions that address the prevention of interruptions to business activities and the timely resumption. It includes procedures to address recovery of electronic data from loss, damage, theft or compromise and includes plans for all of the Company's critical business processes, physical facilities and equipment. Specific timelines for tasks to be completed and services recovered are outlined in the Disaster Recovery Plan and are prioritized by order of importance.

The Disaster Recovery Plan has been distributed to all employees that may be called upon to play an active role during an emergency situation. These employees, and their roles for executing the plan during a disaster recovery event, are further outlined within the Disaster Recovery Plan.

The Company's Disaster Recovery plan includes current contact information for all employees, contractors, vendors, and clients. It is the responsibility of the Company President or their designee to keep the Disaster Recovery Plan's contact information updated at all times.

The Disaster Recovery Plan includes a schedule of tasks and list of services (in order of priority) to be recovered. It also contains information regarding the testing schedule of the plan, including types of tests that may be performed and the frequency for which testing is completed. Documentation of testing performed for the Disaster Recovery Plan is included within the policies and procedures of the plan.

3.8.1 – Disaster Recovery Plan

Shield Title AZ ('the Company") has adopted the Business Continuity and Disaster Recovery procedures outlined herein as part of the Company's Information Security Program located in Appendix B. These procedures are in place to assist the Company in a timely resumption of business activities should it experience an unexpected information system failure, including emergency or disaster situations.

BEST PRACTICE FOUR (4) – SETTLEMENT POLICIES AND PROCEDURES

Definition: ***Adopt standard real estate settlement policies and procedures that help ensure compliance with Federal and State Consumers Financial laws as applicable to the settlement process.***

Shield Title AZ Policy and Procedures: Shield Title AZ use of software and technology allows us to track a file through each step of the closing process and provide complete transparency of the work being done on each file. As such we are able to verify that each part of the closing process adheres to accurate company procedures and that check and balances are in place to monitor these procedures. These include:

- Obtaining proper information required prior to closing
- Up to date access to premium rate information
- Complete review of closing instructions
- Proper processing of mortgage payoffs
- Accurate disbursement of proceeds and handling of escrow funds
- Timely and accurate recording guidelines
- Conducts an updated title search prior to settlement

4.1 – RECORDING PROCEDURES

Shield Title AZ ("the Company") has procedures to ensure the timely recording of all documents related to settlements conducted by the Company. These procedures meet all legal and contractual obligations as well as State, Federal, local, and industry standards and regulations that govern the settlement process.

The Company issues title insurance policies in connection with settlements conducted by the Company. The Company is responsible for the recording of all documents from the settlements it conducts.

Documents that need to be recorded from each settlement are delivered to the appropriate governmental office within forty-eight (48) of settlement or disbursement. Prior to such delivery the following procedures are followed:

1. Drafts of all documents (Deeds, Mortgages, etc.) that need to be executed and recorded pursuant to the title insurance commitment are reviewed and proofed by the President prior to settlement for the following:

- Documents are in appropriate format (size, margins, etc.) and correct order for the County/State;
- Document Date;
- Amount of Consideration;
- Names of grantee, grantor, mortgagor, mortgagee, etc.;
- Marital status of all natural persons;
- T enancy;

- Representative capacity of individuals signing on behalf of entities;
- POA, Trust, Probate, Estate language, if applicable;
- Legal Description of the property;
- Parcel I.D.;
- Signatures and Witnesses;
- Notary/Acknowledgement clauses are complete and accurate;
- Return to name and address;
- Riders;
- Attorney/Preparer Certification;
- Affidavits

Any errors or omissions discovered with the document drafts are corrected prior to settlement.

2. Upon completion of each settlement conducted by the Company, the entire file is returned to the President along with the check(s) for recording fees, recording taxes and transfer taxes.

3. Within twenty-four (24) hours of settlement, the President reviews all of the executed documents to make sure they are the same as the drafts that were approved; that they were fully and properly executed and that they are ready for recording.

4. The President reviews the check(s) to make sure the payees and amounts are correct.

5. If any errors or omissions are discovered with the documents or checks, immediate measures taken to correct them.

6. Upon approval of the documents and check(s), copies are made for the file and transmitted daily by overnight courier with a return envelope to the appropriate county recorder's office.

7. The Company tracks all documents sent for recording to ensure timely recording. The Company retains all files during the recordation process in a designated locked file cabinet. Entries are made to the Document Recording Log and tracked daily by the President.

The President monitors/reviews the outstanding check list and custom reports generated from CPA Software reconciliation software that identifies recording checks outstanding for more than ten (10) days. The President contacts the county recorder's office for any file not return within the normal business cycle. The President requests a Post-Closing update (rundown) to the title search to verify proper recordation and indexing and to determine any intervening matters exist.

8. If a document is rejected for any reason, it is returned immediately to the President who takes the necessary measures to correct the problem within two (2) business days. Once the

problem has been corrected, the document is resubmitted without delay and in no case, no more than thirty (30) days.

9. All documents are returned to the Company after recording and delivered to the President. The President reviews the recorded documents to make sure they were recorded in the proper order and properly indexed by the Courthouse.

10. Copies of the documents with the recording stamps (date, time, book and page/instrument no.) are made for the file.

11. The policies and documents are prepared for delivery to the insured in accordance with procedure reference no. 5.1 herein.

12. The Company President reviews the Company's Document Recording Log monthly to ensure all documents are recorded. Any exceptions are addressed and resolved immediately.

4.2 – PRICING PROCEDURES

Shield Title AZ ("the Company") has procedures to ensure that customers are charged the correct title insurance premium and other charges for settlement services provided by the Company. Premiums and charges for services are determined by legal and contractual obligations as well as State, Federal, local, and industry standards and regulations which govern the settlement process.

1. The Company's Closers prepare the HUD-1 Settlement Statements and are responsible for ensuring the correct title insurance premium is charged for each transaction. At all times, Closers maintain access the company's Epic Software settlement software and to the Underwriter's on-line rate calculator as well as complete copies of the current underwriter's Rate Manual(s). They are familiar with premiums, rules and discounts. Upon notification from the state or an underwriter that changes have been made to the Rates, the Closers are immediately provided with the new Rate Manual and the Company's settlement service software vendor is contacted to confirm they have updated their software.

2. The Company's underwriter's rates are incorporated into the Company's Epic Software Desk Top settlement service software. The rates are identical to the ones provided to the settlement service software vendor by the underwriter. The software calculates the policy premium based on the policy types, amounts, rate type and endorsements entered by the Closer.

3. The Closers also utilizes the underwriter's online rate calculator program to determine/double check the proper charges to collect on the HUD-1 settlement statement for the policy(ies), endorsements and Closing Protection Letter, if any. A printout from the settlement software or underwriter's online rate calculator program is maintained in the file to document the calculation.

4. Prior to settlement, each buyer/borrower is provided with notice of any Reduced Rates which provides them with notice of documentation that will entitle them to a reduced rate if the documentation is provided to the Company prior to settlement. If the buyer/borrower provides such documentation prior to settlement, the Closer ensures that the applicable reduced rate is charged on the HUD-1 settlement statement. The settlement software's rate calculator program is utilized to verify the calculation and a printout is maintained in the file to document the calculation.

5. The Company's Closers are also responsible for ensuring all additional fees the Company collects for services (i.e. – Settlement Fee, Overnight Delivery, Wire Fees, Tax Certifications, Notary) are correctly charged for each transaction. Fees payable to third party service providers are charged in accordance with the third party service provider's invoice.

6. A post-settlement review of charges is performed by the Office Manager when preparing the monthly premium report of remittances due to the underwriter. If any over-charges are discovered, the Office Manager has the Company President review the file. If the Company President confirms there was an over-charge, a refund check is issued immediately and same is documented in the file.

7. If the Company's underwriter notifies the Company of an over-charge discovered during their processing of premiums and/or policy copies, the Company immediately issues a refund check and documents same in the file.

4.3 – RECORDING AND PRICING TRAINING

Shield Title AZ ("the Company") has policies and procedures relating to document recording and pricing of title insurance policies and settlement services to ensure a settlement process that is compliant with legal and contractual obligations as well as State, Federal, local and industry standards and regulations. All employees involved in the settlement process shall undergo initial and ongoing training with respect to the Company's recording and pricing procedures.

New employee training: All employees hired by the Company will undergo specific training programs including:

- Document recording policies and procedures;
- Pricing policies and procedures

New employees whose duties will include recording functions will have additional training on specific recording functions, including the use of recording checklists. These employees are given a copy of all the Company's recording policies and procedures, and recording checklists before they begin performing these duties for the Company.

New employees whose duties will include pricing functions, including post-closing rate/fee pricing verification functions, will have additional training on quality control checks and other rate pricing guidelines. These employees are given a copy of all the Company's policies and procedures, and will receive specific training on rate manuals and online calculators utilized by the Company before they begin performing these duties for the Company.

BEST PRACTICE FIVE (5) – TITLE PRODUCTION

Definition: ***Adopt and maintain appropriate procedures for the production, delivery, reporting and remittance of title insurance policies designed to meet both legal and contractual obligations.***

Shield Title AZ Policy and Procedures: Shield Title AZ policy is to deliver all policies to customers within the guidelines set forth by the underwriters' agency contracts (generally by the end of the first full month following closing). Policies are prepared and delivered following review that all terms and conditions of the title insurance commitment have been satisfied and all closing documents and necessary releases have been recorded. The Company is an authorized title insurance agency/agent for ATGF (Attorneys Title Guarantee Fund)

5.1 – TITLE POLICY AND DELIVERY PROCEDURES
Shield Title AZ ("the Company") shall issue and deliver all title insurance policies to the insured parties within thirty days of the later of (i) the date of settlement, or (ii) the date that the terms and conditions of the title insurance commitment are satisfied.

DAILY PROCEDURES

1. A title insurance commitment must be prepared and delivered to all proposed insured parties before settlement is conducted and any title insurance policy is delivered to them. When the Company is conducting settlement in connection with the transaction, the commitment is delivered at least five business days prior to settlement.

2. All title insurance commitments are prepared after a careful examination of the title and determination of insurability in strict accordance with the Company's underwriter guidelines by one of the Company's authorized signatories.

3. Settlement may be scheduled and conducted once the Company is satisfied that all commitment requirements have been met or will be met at settlement.

4. After settlement is conducted, the file is reviewed by the Closer immediately after disbursement of the settlement funds.

5. The commitment is marked-up by the Closer to identify which requirements and exceptions on Schedules B-I and B-II have been satisfied and which ones will remain on the final policies as exceptions.

6. If additional documentation is needed for any of the commitment requirements, the file processor works to obtain same.

7. Once all of the requirements on Schedule B-I have been marked-up as being satisfied, the Office Manager reviews the title insurance policy section of the loan closing instructions; generates the necessary policy jackets via the underwriter's online system and prepares the policy schedules and endorsements in accordance with the loan closing instructions.

8. After the policies are prepared, the Office Manager signs the policy or gives the entire file to an authorized policy signatory. Within five days of receiving the file, the authorized signatory reviews the file along with the prepared policies. If there are any issues detected by the authorized signatory, they will meet with the Closer to resolve them.

9. Once the authorized signatory is satisfied that the file is complete and all of the title insurance commitment conditions and requirements have been met, the policies and endorsements are signed and the file is then returned to the Office Manager.

10. The Office Manager types cover letters to be sent to the insured parties with the original policies and original, recorded insured instruments (Deeds and/or Mortgages).

11. Two copies of the policies and endorsements are made. One copy is maintained in the file, the other copy and it is placed a secure file labeled "Underwriter Policy Copies" which contains copies of all policies issued during the month.

12. The original, recorded Deed and Owner's Policy, if any, are mailed to the purchaser.

13. The original, recorded Mortgage and Loan Policy are overnighted to the address provided in the loan closing instructions. The tracking number of the overnight package is maintained in the file.

Note about ALTA Short Form Residential Loan Policies:
If the property is a One-to-Four Family Residence and the lender's closing instructions call for an ALTA Short Form Residential Loan Policy; the policy is typed, reviewed and signed immediately after settlement and sent to the lender with the closing package in accordance with the loan closing instructions.

MONTHLY PROCEDURE

The Office Manager monitors policy issuance via reports from the Company's settlement software and its underwriter to ensure compliance with these procedures.

5.2 – PREMIUM REMITTANCE AND POLICY REPORTING PROCEDURES

Shield Title AZ ("the Company") shall report all title insurance premiums and policies to the underwriter(s) within the time frame required by the underwriter agency contract(s) and within the time frame required by any state statute or regulation.

DAILY PROCEDURES

1. Whenever a settlement is conducted in connection with a title insurance commitment issued by the Company, a check payable to the title insurance underwriter for their portion of the policy premium, endorsement premium(s), if any, and Closing Protection Letter fee, if any, is cut when the file is disbursed. The check is kept in the file and both are returned to the file processor.

2. The Office Manager enters the policy details in the underwriter's Monthly Premium Report ("MPR") system; ensures that the check amount matches the calculation by the underwriter's system. The Office Manager places the check in a secure file labeled "Underwriter Remittance" which contains all checks made payable to the underwriter during the month.

MONTHLY PROCEDURES

1. During the first week of each month, the Company President prints a report of all title insurance settlements conducted the previous month along with the underwriter's MPR system report for that month. The Company President compares the two reports to each other to make sure there are no discrepancies then compares the checks in the "Underwriter Remittance" file to the reports to make sure all files and checks are accounted for.

2. The Company President compares each check in the Underwriter Remittance file to the underwriter's MPR system report to make sure each check amount matches the MPR system calculation. The Company President also sums up all of the checks to make sure the total sum matches the total on the MPR report. Any differences are researched and corrected.

3. Having confirmed all of the title insurance files from the previous month are included on the underwriter's Monthly Premium Report and all of the checks are for the correct amounts, the bookkeeper prepares an overnight package with Monthly Premium Report and checks. The bookkeeper then gathers all of the policy from the Underwriter Policy Copies file; creates a list of the file numbers and policy numbers then places the copies in the overnight package as well.

4. The policy copies, Monthly Premium Report and checks are overnighted to the underwriter so that they receive it by the last day of the month.

5. The Company President places copies of the Monthly Premium Report, policy copy list and overnight air bill in a file containing the underwriter's name and year.

6. If the underwriter contacts the Company with any questions or additional documentation requests, the Company President addresses same within 48 hours.

QUARTERLY PROCEDURES

The Company President reviews a Policy Status Report and a Premium Variance Report from the underwriter to make see if there are discrepancies that need to be reconciled. Files shown as not reported yet are researched to determine if they are canceled or still pending. Any file determined to have been canceled is then reported as such to the underwriter. Any discrepancies shown on the premium variance report are researched and rectified, if necessary.

BEST PRACTICE SIX (6) – ERRORS AND OMISSIONS, FIDELITY, AND CYBER LIABILITY COVERAGE

Definition: ***Maintain appropriate levels of professional liability and fidelity coverage to ensure the financial capacity to stand behind the professional services provided.***

Shield Title AZ and Procedures: Shield Title AZ consistently maintains all levels of insurance as required by underwriters and lenders and that is comparable to the complexity, nature and scope of our operations. Coverage is held for professional liability and fidelity coverage (including employee theft) as well as any additional bond coverage that may be required by the state of Arizona.

6.1 – E & O INSURANCE RENEWAL PROCEDURES

Shield Title AZ ("the Company") shall maintain appropriate levels of Professional Liability/Errors & Omissions Insurance to ensure the Company has the financial capacity to stand behind its professional services and to ensure compliance with state regulations and underwriter agency contracts.

The Company has a current Professional Liability/Errors & Omissions Policy insured through BiBERK with an effective date of 05/11/2022 and an expiration date of 05/11/2023. The policy's retro-active date is 05/11/2022. The policy limits are $ 1,000,000 each claim and $1,000,000 aggregate. The deductible amount is $2,500. The policy specifically includes Title Agent, Closing Agent and Escrow Agent in the definition of "professional services."

ANNUAL PROCEDURES

1. The Company President maintains a complete copy of the policy in a secure file in their office. Sixty days prior to the expiration date of the policy, the Company President reviews the

applicable state regulations and underwriter agency agreement(s) to determine if any requirements have changed.

2. The Company President reviews the definition of "professional services" in the policy to determine if the policy provides adequate coverage for the Company's current scope of operations. Any additional coverage deemed necessary is requested at the time of renewal.

6.2 – FIDELITY/SURETY BOND RENEWAL PROCEDURES

Shield Title AZ ("the Company") shall maintain a Fidelity/Surety Bond to provide coverage for employee dishonesty/crime in compliance with any state regulations and underwriter agency agreements. Currently, the state of Arizona or its underwriters require licensed title agents (producers) to maintain a Fidelity/Surety Bond (employee dishonesty coverage) but the Company recognizes the importance of maintaining the coverage.

The Company has a current FidelitySurety Bond #0815468 through Harco National Insurance Company in the amount of $100,000 with an effective date of 04/11/2022 and an expiration date of 04/11/2023. The deductible amount is $1,000.

ANNUAL PROCEDURES

1. The Company President maintains a complete copy of the Fidelity Bond in a secure file in their office. Sixty days prior to the expiration date of each Bond, the Company President reviews the applicable state regulations and underwriter agency agreements to determine if any requirements have changed.

2. After reviewing the applicable state regulations, underwriter agency agreements and existing Bonds, the Company President completes renewal applications at least thirty days prior to the expiration of the current Bonds.

6.3 CYBER LIABILITY INSURANCE

Shield Title AZ maintains one policy of Cyber Liability Insurance to provide coverage for data breaches and data theft in compliance with any state regulations and underwriter agency agreements. Shield Title AZ's Cyber Liability Insurance policy is through The Hartford in the amount of $,1000,000 with an effective date of 05/11/2022 and an expiration date of 05/11/2023. The deductible amount on Cyber Liability policy from The Hartford policy is $10,000.

A. ANNUAL RENEWAL PROCEDURES

1. The Company General Counsel maintains a complete copy of the Cyber Liability policies in a secure file in their office. Sixty (60) days prior to the expiration date of each Cyber Liability

policy, the Company General Counsel reviews the applicable state regulations and underwriter agency agreements to determine if any requirements have changed.

2. After reviewing the applicable state regulations, underwriter agency agreements and existing policies, the Company General Counsel completes renewal applications at least thirty (30) days prior to the expiration of the current Cyber Liability policies.

BEST PRACTICE SEVEN (7) – CONSUMER COMPLAINTS

Definition: ***Adopt and maintain procedures for receiving and addressing consumer complaints so that any instances of poor service or non-compliance do not go undiscovered.***

Shield Title AZ Policies and Procedures: Shield Title AZ is very sensitive to any complaints that are made. Any and all complaints received by an employee are to be forwarded to our Company President for immediate resolution. This resolution will always include a follow up to not only the customer but also their loan officer to ensure that it is agreed that the issue has been resolved. In certain cases, the complaint is discussed with an employee regarding the circumstances causing the complaint and a review of Shield Title AZ policies and procedures. All activity is logged and placed in the corresponding transactional file.

7.1 – CONSUMER COMPLAINT INTAKE, RECORDATION AND RESPONSE PROCEDURES

Shield Title AZ ('the Company") is dedicated to providing excellent client satisfaction and customer service. In an effort to ensure that complaints are addressed as efficiently and effectively as possible, the Company has a written Consumer Complaint Policy and procedures for the intake, recordation and response to client and customer complaints.

The Company has a written Consumer Complaint Policy that all employees must follow to ensure an effective and consistent way for dealing with client and customer complaints. The policy is made available to customers at settlement.

The written Consumer Complaint Policy is reviewed annually by all employees.

The definition of the term complaint is defined under the Complaint Resolution Policy as an expression of dissatisfaction or concern expressed by a client or customer regarding the services, operating procedures, staff, vendors, or complaint handling process.

1. Each complaint received is directed to the Company President who completes a Complaint Intake Form that includes:

- Date of complaint;
- Contact information of the consumer or person making the complaint;
- File number; name and/or policy number;
- Brief description of the complaint;
- Brief description of the resolution requested;
- Amount of fees associated with the transaction (if complaint is related to fees);
- Employee assigned to;
- Summary of Resolution;

2. The Company President also logs all complaints on the Company's Consumer Complaint Log which is used to identify open complaints.

3. The Company President assigns an employee to investigate and resolve each complaint within 24 hours of receipt.

4. The designated employee is provided with a copy of the Complaint Intake Form.

5. The designated employee locates the relevant file(s); reviews the relevant documentation; determines a proper resolution and carries out the action(s) necessary to resolve the complaint.

6. In the event that the employee is unable to resolve the complaint to the customer's satisfaction, the Company President will review the matter and re-assign it or assume the responsibility.

7. Upon resolution of the complaint (or inability to resolve), the employee completes the Summary of Resolution section of the Intake Form and returns it along with the supporting documentation, if any, to the Company President.

8. Complaint records are retained for a period of 5 years.

7.2 – COMPLAINT RECORDS PROCEDURES

Shield Title AZ ('the Company") is dedicated to providing excellent client satisfaction and customer service. In an effort to ensure that complaints are addressed as efficiently and effectively as possible, the Company records all complaints and tracks them. Lenders will be permitted to see complaint records related to their loans.

All complaints received by the Company are logged on the Company's Consumer Complaint Log which is used to track the status of each complaint.

The Log is maintained by the Company President.

7.3 – ANALYSIS AND SELF-ASSESSMENT PROCEDURES

Shield Title AZ ('the Company") is dedicated to providing excellent client satisfaction and customer service. In an effort to ensure that complaints are addressed as efficiently and effectively as possible, the Company reviews and analyzes the handling of complaints so adjustments to operations and procedures can be made as warranted.

The Company President and Company President review and analyze the Company's handling of consumer complaints in accordance with the Company's written consumer complaint policy on a semi-annual basis.

The purpose of the semi-annual review is to identify trends and types of risks (i.e. – legal, regulatory, reputation, financial, etc.) to determine if any changes need to be made to the Company's policies and procedures.

7.4 – CONSUMER COMPLAINT TRAINING PROCEDURES

Shield Title AZ ('the Company") is dedicated to providing excellent client satisfaction and customer service. In an effort to ensure that complaints are addressed as efficiently and effectively as possible, all employees receive annual training on the Company's Consumer Complaint Policy.

New employee training: All employees hired by the Company will undergo specific training programs including:

- Consumer Complaint Policy
- Complaint Intake, Recordation and Response;
- Investigating and Resolution

New employees are given a copy of all of the Company's policies and procedures, including a copy of the Company's Complaint Resolution Policy. An acknowledgment of receipt and comprehension of these procedures will be executed by the employee and maintained by the Company President.

All employees will be provided with updates to policies and procedures, including the Company's Complaint Resolution Policy, immediately after the updates are made to the policies and procedures. Employees will receive training, at least annually, on the Company's Complaint Resolution Policy and each employee will complete a training acknowledgment form every time an updated training session is completed. A Complaint Resolution Training Log of the trainings will be maintained by the Company President.

APPENDIX

AVAILABLE UPON REQUEST