INDEPENDENCE TITLE COMPANY

Best Practice Policies

VERSION 1.2

Independence Title

Explore www.IndependenceTitle.com

Table of Contents

Best Practice Policies Version 1.2

LICENSING

ALTA Best Practice No. 1: Establish and maintain current license(s) as required to conduct the business of title insurance and settlement services.

Purpose: Maintaining state-mandated insurance licenses and corporate registrations helps ensure the Company remains in good standing with the State.

Company Policies and Procedures for Implementation and Adherence to Best Practice No. 1:

1. Licensing

    a. The Company has established and will maintain its license as required to conduct the business of title insurance and settlement services.

    b. The Company will maintain compliance with other licensing, registration, or similar requirements with the applicable state regulatory department or agency, including the Texas Department of Insurance.

    c. All fees associated with licensing will be paid by the Company.

2. All required licenses, state regulatory licenses, registrations or similar requirements are documented by the Company in a Company directory, which contains the following information: licensee name, license type, license number and expiration/renewal date.

3. The Company's licensing status is reviewed and updated at a minimum of annually to ensure accurate and timely tracking and renewal of licenses.

4. The Company shall remain in good standing with the Texas Secretary of State by filing any required forms and supporting documentation regarding the business of the Company.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

5. The Company shall monitor and oversee mandatory continuing education credits for its employees, in order to maintain appropriate licenses. Continuing education credit information shall be provided to employees by the Company's administrative staff. All employees are required to keep up with the number of hours they have completed toward the total requirement of continuing education hours necessary per relevant license period(s).

6. The Principals and Employees of the Company shall:

    a. Maintain the necessary qualifications and requirements to obtain and maintain each required license.

    b. Pay, in a timely manner, any and all fees necessary to maintain each required license.

    c. Perform any and all professional training necessary to maintain each required license.

7. Each Licensee that fails to perform all of the requirements necessary shall be prohibited from performing such functions for which the license is required, until such time as the license is restored.

ESCROW ACCOUNTS

ALTA Best Practice No. 2: Adopt and maintain appropriate written procedures and controls for Escrow Trust Accounts allowing for electronic verification of reconciliation.

Purpose: Appropriate and effective escrow controls and staff training help title and settlement companies meet customer and legal requirements for the safeguarding of customer funds. These procedures help ensure accuracy and minimize the exposure to loss of client funds. Settlement companies may engage outside contractors to conduct segregation of trust accounting duties.

Company Policies and Procedures for Implementation and Adherence To Best Practice No. 2:

In addition to following all applicable laws concerning trust accounting, the Company shall follow all of the following policies and procedures regarding escrow accounts.

1. Authorized Employees Only

    a. Only those employees whose authority has been defined to authorize bank transactions may do so.

    b. Appropriate authorization levels shall be set for employees by the Company and reviewed for updates annually.

    c. All employees with access to escrow funds or Non-public Personal Information (NPI) shall undergo criminal background checks going back a minimum of five years upon or prior to hiring, which shall be passed upon legal and licensing requirements and job functions.

    d. At least every three years, employees with access to escrow funds or NPI shall undergo subsequent criminal background checks going back a minimum of five years, which shall be passed upon legal requirements and job functions.

    e. Ongoing annual training shall be performed for all employees with access to entrusted funds or NPI, regarding the proper management of the escrow accounts.

f. Former employees shall be immediately deleted as listed signatories on all bank accounts, and divested of all computer access privileges to the Company network and/or any online banking functions.

g. Access to escrow funds shall be limited on a basis of necessity. Accordingly, employees shall be granted the minimum amount of access necessary for their job functions.

h. The Company shall conduct periodic reviews of all user access rights, with review of privileged access rights to occur more frequently. Appropriate procedures shall be implemented to prevent unauthorized access to the Company operating systems, and the data and services thereof.

i. All data systems permitting access to electronic banking shall require users to log-in with their assigned User ID and password before obtaining access. Whenever possible, operating systems shall include appropriate technological controls to shut down and "lock out" the user after a defined period of inactivity, and require re-authentication by the user before the interactive session may be resumed. The strictness of such controls shall be commensurate to the risks associated with the type of user and the sensitivity of the relevant information. Where such controls are impracticable or incompatible with a particular business process, other appropriate controls shall be implemented to reduce vulnerabilities.

2. Escrow Accounts Maintained At Insured Banks

   The Company shall maintain all escrow accounts at federally insured financial institutions. If directed in writing by the beneficial owner of certain funds to be held in escrow, the Company may put those funds (and only those funds) in a separate account with an institution designated by the beneficial owner of said funds.

3. Anti-Fraud Corruption Policy

   a. Fraud and corruption will not be tolerated by the Company, either within the Company or in conjunction with, or targeted towards Company employees, customers, partners, suppliers or vendors.

i. All reports for suspected fraud, corruption, or related misconduct must be made in good faith, and retaliation and retribution will not be tolerated.

ii. Persons who make reports which are malicious, knowingly false, or unjustly likely to damage another employee's reputation may face disciplinary action.

b. When fraud or corruption is suspected or detected, sufficient resources shall be employed to gather evidence to support:

i. disciplinary action

ii. prosecution

iii. recovery of losses and costs

Company will determine, in its own discretion, what actions might be appropriate for those involved in the fraud or related misconduct, according to federal and state employment laws.

c. Preventative measures:

i. Fraud prevention accounting procedures are in place, applicable to escrow account reconciliations, cash management, credit card usage and commercial transactions

ii. Background checks will be required as set forth herein.

iii. Continued training and education on fraud prevention and detection will be required

d. Risk Assessments:

On as-needed, but no less often than annual basis, Company administrative staff, in consultation with department managers will review the effectiveness of the Anti-Fraud Corruption Policy as well as Company's susceptibility to fraudulent or deceptive practices

e. Responsibilities of employees

   All employees shall:

   i. Understand and follow all preventative procedures

   ii. Assist with prevention and detection of fraud, corruption or related misconduct

   iii. Report suspected fraud, corruption, or related misconduct

f. Company shall cooperate with the police or appropriate governmental agencies in any investigation of suspected fraud or corruption.

4. Separation of Accounts

   a. The Company shall maintain a separate escrow account for real estate transactions.
   b. Regardless of how many escrow accounts are maintained by the Company:
      i. Company funds and escrow funds shall NOT be commingled.
      ii. Operating accounts are to be separately maintained from all escrow funds, and properly identified including, but not limited to, checks, deposit slips, ledgers, statements and all related supporting documentation.
      iii. Escrow accounts are to be separately maintained from all Company funds and properly identified, including, but not limited to, checks, deposit slips, ledgers, statements and all related supporting documentation.
   c. Escrow funds or any other funds which the Company maintains under escrow agreement shall NOT be commingled with an employee's, manager's, or principal's personal account.
   d. Escrow Trust Accounts are to be properly identified as "escrow" accounts.

5. Separation of Duties

   The Company shall:

a. Separate the check writing and check signing authority and functions between two authorized employees and/or principals of the Company where required by state regulation.
b. Separate the wire preparation and wire initiation authority and functions between two authorized employees and/or principals of the Company where required by state regulation.
c. Separate the escrow account reconciliation authority and functions from the check signing and wire initiation authority and functions.

6. General Governing Rules

The Company shall:

a. Use International Wire Blocks, to prevent any wires from the escrow accounts without additional authorization, if available.
b. Use Automated Clearing House Blocks to prevent any ACH Transactions from the escrow account without additional authorization, if available.
c. Use Positive Pay and/or Reverse Positive Pay to verify the issuance of a check at the bank before clearing said check, if available.
d. Utilize a Zero Balance escrow account for external distribution on incoming wires which are swept into the escrow accounts.

7. Reconciliation of Escrow Trust Accounts

a. Escrow accounts are to be prepared with trial balances.
b. Outstanding file balances shall be documented.
c. Each transaction in an escrow account shall balance. Negative balances shall not be permitted.
d. Segregation of duties shall be in place to ensure the reliability of the reconciliation and reconciliations shall be conducted by someone other than those with signing authority.
e. Reconciliation standards:
    i. All escrow accounts shall be reconciled.
    ii. Receipts and disbursements shall be reconciled every day.
    iii. Opening balance for the month shall match the ending balance for the prior month's reconciliation.
    iv. On at least a monthly basis, escrow accounts shall be prepared with Trial Balances ("Three-Way Reconciliation"), listing all open escrow balances.

IMPORTANT: the Three Way Reconciliation documentation, at a minimum, includes bank statement, reconciliation sheet or summary page with book balance, outstanding deposits list/deposits in transit, open escrow file listing or trial balance, and outstanding disbursements list all as of the reconciliation date. All amounts should be equal between the book balance, reconciled bank balance and trial balance.

v. Within thirty (30) days of the receipt of the bank statement, the Company shall perform the Three-Way Reconciliation.
vi. Within ten (10) days of the discovery of an open exception, the Company shall resolve any and all open exceptions or document a reason for the exception remaining open.
vii. Within ten (10) days of the completion of the Three-Way Reconciliation, the Company shall resolve any and all open exceptions or document a reason for the exception remaining open.
viii. In no event shall an exception remain unresolved or unexplained from one Three-Way Reconciliation to the next.
ix. Within thirty (30) days of the completion of the Three-Way Reconciliation, the Three-Way Reconciliation shall be reviewed by a senior executive of the Company.

f. The results of the Three-Way Reconciliation shall be available and electronically accessible upon request for audit purposes by the Company's contracted title underwriter.

8. Payment of Bank Fees on Escrow Accounts

Bank fees for the escrow accounts shall be paid out of the Company's operating account and not the escrow account.

PRIVACY AND PROTECTION OF NON-PUBLIC PERSONAL INFORMATION

Best Practice No. 3: Adopt and maintain a written privacy and information security program to protect Non-public Personal Information as required by local, state and federal law.

Purpose: Federal and state laws (including the Gramm-Leach-Bliley Act) require title companies to develop a written information security program that describes the procedures they employ to protect Non-public Personal Information. The program must be appropriate to the Company's size and complexity, the nature and scope of the Company's activities, and the sensitivity of the consumer information the Company handles. A Company evaluates and adjusts its program in light of relevant circumstances, including changes in the Company's business or operations, or the results of security testing and monitoring.

Company Policies and Procedures for Implementation and Adherence To Best Practice No. 3:

1. Administrative Responsibility

   The Company's administrative staff shall be responsible for coordinating and overseeing all matters regarding the protection of Non-public Personal Information (NPI) and this Best Practice No. 3. Senior executives of the Company may designate other representatives of the Company to oversee and coordinate particular elements of this Policy. Any questions regarding the implementation or interpretation of this Policy shall be directed to the administrative staff of the Company.

2. Risk Identification and Assessment

   The Company recognizes that it is subject to both internal and external risks regarding the security of NPI. These risks include, but are not limited to:

   a. Unauthorized access to Non-Public Personal Information (NPI) within the Company records by employees, third party service

providers, vendors, couriers, or other persons or service providers with whom Company does business

b. Unauthorized requests for access to the Company records
c. Interception of data during transmission
d. Loss of data in a natural disaster
e. Corruption of data or technology systems
f. Misplacement or loss of paper records
g. Compromise of data from disposal of documents, records or equipment
h. Unauthorized or unintended disclosure of electronic or printed NPI
i. Failure to adequately monitor third party service providers and risks that third party providers could improperly make use of NPI
j. Risks relating to the fact that the Company relies on an outside vendor to manage its network and information technology systems
k. Remote access to the Company's private network
l. Access to the Company's private network and resources
m. Employees transmitting unencrypted NPI through electronic mail, computer software programs or any third party digital system

The Company intends, as part of this Policy, to conduct a review on an annual basis, to identify and assess external and internal risks to the security, confidentiality, and integrity of NPI that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information.

Areas to be reviewed may include: employee training and management; information systems, including network and software design; information processing, storage and disposal; detecting, preventing and responding to attacks, intrusions or other system failures.

3. Privacy Assessment

The Company's administrative staff shall:

a. Assess the risks to NPI associated with the Company's information systems, including network and software design, information processing, and the storage, transmission and disposal of NPI.

b. Assess procedures for monitoring potential information security threats associated with software systems, and assess procedures for updating such systems by implementing patches or other software fixes designed to deal with known security flaws.

c. Evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures, and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies.

4. General Background Investigations Policy

a. Background checks will be conducted by Company in accordance with the concepts of using industry-recognized agencies and sources, in accordance with federal and state laws.
b. Background checks will be done on all employee candidates upon or prior to hiring, and when appropriate, on contractors, sub-contractors, consultants and temporary employees
c. Additionally, background checks are mandatory for all employees who hold or are being considered for positions that include financial responsibilities and/or access to NPI.
d. Cooperation and compliance with this Policy is a condition of employment or continued employment with the Company. Refusal may result in disqualification from employment with the Company
e. Company shall maintain and store all background investigation documents for a period of not less than three years to verify background investigations were performed on candidates in compliance with this Policy.

5. Employee Training, Management and Responsibilities

a. Employee Training

i. A member of the Company's administrative staff shall explain to incoming employees and temporary contract personnel their responsibilities under this Policy, as well as other

applicable security policies and procedures, and the potential consequences of non-compliance.

ii. Each new employee will receive appropriate training regarding the importance of information security and NPI during orientation, including the proper use of computer information and passwords. Appropriate training includes controls and procedures to prevent employees from providing NPI to unauthorized parties, and methods for proper disposal of documents containing NPI. In the case of temporary workers, a supervisor will provide adequate training regarding the identification and protection of NPI to protect against disclosure.

iii. New employees and temporary contract personnel will receive a copy of this Best Practice Policy as part of the hiring process and must make attestation that they have read and understood the Policy.

iv. Supervisors of activities that use NPI must be particularly vigilant in ensuring their employees understand and have adequate training in data privacy and information security.

v. At least annually, the Company will provide training to all employees to remind them of the importance of information security and to ensure that the safeguarding procedures and controls are followed. Training activities may be modified depending on the risks perceived, scope and types of activities, and access to NPI.

b. Employee Management

i. All employees with access to NPI or escrow accounts shall undergo criminal background checks upon or prior to hiring, going back a minimum of five years, which shall be passed upon legal requirements and job functions.

ii. At least every three years, all employees with access to NPI or escrow funds shall undergo subsequent criminal background checks going back a minimum of five years,

which shall be passed upon legal requirements and job functions.

iii. Access to NPI shall be limited on a "need-to-know" basis. Accordingly, employees shall be granted the minimum amount of access necessary for their job functions.

iv. The Company shall conduct periodic reviews of all user access rights, with review of privileged access rights to occur more frequently. Appropriate procedures shall be implemented to prevent unauthorized access to the Company operating systems, and the data and services thereof. Access to NPI shall be limited to authorized users through the use of authentication procedures.

v. All data systems permitting access to NPI shall require users to log-in with their assigned User ID and password before obtaining access. Whenever possible, operating systems shall include appropriate technological controls to shut down and "lock out" the user after a defined period of inactivity, and require re-authentication by the user before the interactive session may be resumed. The strictness of such controls shall be commensurate to the risks associated with the type of user and the sensitivity of the relevant information. Where such controls are impracticable or incompatible with a particular business process, other appropriate controls shall be implemented to reduce vulnerabilities.

vi. Access privileges must be immediately reviewed and adjusted (expanded or decreased) any time a Company employee is terminated or changes job functions, as well as any time an independent contractor, fee attorney office, or third party service provider severs its relationship with the Company. Upon termination of employment or severance of a relationship with a fee attorney office, contractor or third party, all access to Company computer systems must be promptly removed and discontinued.

vii. All hardware and software assets assigned to an employee, contractor, or third party user must be returned upon

separation from the Company or termination of the engagement.

viii. The Company may implement additional termination and separation procedures as appropriate to ensure the security of NPI.

c. Employee Responsibilities

The Company expects all employees to exercise good judgment regarding their use of Company networks and information technology resources. In particular, employees are required to maintain authentication security (*i.e.* passwords and access tokens) and to secure computers and other office equipment.

i. Each employee:

A. Is personally responsible for the usage of his or her User ID and password.

B. May not store passwords on computer systems in unprotected form, and may not write passwords down unless stored in a secure location away from their computers.

C. Is further prohibited from "loaning" or otherwise disclosing their passwords to others and from using the passwords of other users.

D. Who suspects his or her password has been compromised must change the password immediately and report this suspicion.

E. Shall ensure that unattended computing equipment has appropriate protection. The Company requires employees to terminate active (logged-in) sessions before leaving a device unattended, unless it can be securely "locked" (*e.g.*, with a password-protected screensaver). The Company may also require employees to physically secure a device, or the area in

which the device is located, with a key lock or equivalent before leaving it unattended.

6. Information Security

   a. Physical Security

      i. No Unauthorized Access to NPI

      The Company shall not allow unauthorized physical access or damage to NPI. Security measures employed shall be commensurate with the risks and any relevant legal, regulatory, or contractual requirements associated with a particular office space.

      Within Company offices, in particular any housing Company computer data servers, access shall be restricted to individuals whose access is necessary to perform legitimate business functions. The Company shall clearly identify such restricted areas and take additional security measures as appropriate to prevent unauthorized access. Where appropriate, additional security measures may include use of security cameras and logging of visitor entry.

      Company equipment and files stored off-premises shall be protected to the extent possible and appropriate under the circumstances. Appropriate security measures shall be applied for equipment in transit and offsite, taking into account the different risks presented offsite and the sensitivity and value of the information on or accessible through the equipment.

   b. Clean Desk Policy

      The Company strongly encourages observance of a "Clean Desk Policy," as follows:

      i. During the work day, all employees should close or lock electronic files containing NPI on their computers when they are away from their desks.

ii. At the end of the work day, all documents, files, portable devices, and electronic media containing NPI shall be put in a private work area.

c. Restricted Access Model

The Company shall enforce a "Restricted Access Model," as follows:

i. In all Company offices, employees of the Company must accompany any nonaffiliated person(s), including but not limited to couriers, vendors, third party service providers or customers, if the person(s) must pass through an area in the workplace that contains NPI. A "nonaffiliated person" is a person who is not an employee of the Company and who is generally not allowed access to Company records or NPI of Company's customers.
ii. The employee that accompanies the nonaffiliated person(s) shall ensure that there are no inadvertent disclosures of NPI while the nonaffiliated person(s) is/are present in the workplace.

d. Location Security

i. The Company shall institute and maintain physical security for each office, suite, workplace and/or building for every Company location where NPI may be stored.
ii. The Company shall limit and secure points of entry to the building, suite, and any locations where NPI may be stored.
iii. The Company security system includes, where applicable, personal keys/fobs which are used by designated employees to enter their departmental area of the building.
iv. The Company security system also includes an alarm system for each office, suite and/or building as Company determines necessary in each office where Company business is conducted.
v. Security systems will be tested and checked periodically to be sure that an unauthorized entry attempt would be detected, an alarm created, and the incident investigated and resolved.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

7. Network Security

The Company shall take appropriate measures to protect the security of the computer network and NPI in transit. Firewalls shall be used to protect all entry points to the Company networks.

a. Computer Updates

The Company shall keep network and computer systems up to date and take measures to protect Company assets, including NPI, including but not limited to:

i. Maintaining up-to-date operating systems for servers, desktops, laptops and other Company devices that access Company networks.
ii. Applying security patches as suggested by the provider after appropriate validation to ensure any patch will not negatively affect other Company software or processes.
iii. Using Group Policies whenever possible to manage access to network resources, applications, and files which may contain NPI.
iv. Maintaining up-to-date network firewalls.
v. Maintaining up-to-date malware, virus protection and/or spyware, with options to scan removable media.

b. Annual Review and Assessment of Computer Updates and Security Protocols

At least annually, Company may perform independent third-party network security assessments including intrusion detection and penetration testing, and will consider the recommendations of the service provider in ordering updates to keep Company networks protected.

c. Maintain and Secure Access to Company Information Technology

i. Upon adoption and/or subsequent revision of any Best Practice(s), all employees shall read and sign an acknowledgment of the Best Practice policies.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

ii. All employee workstations shall have a setting triggering a password entry requirement after an appropriate period of inactivity (e.g., 15 minutes), at which point a password will be required from the user.
iii. Company wireless networks shall require a password to join.
iv. General password requirements:
    A. Strong passwords shall be required (cannot use birthday or first/last name in a password)
    B. Passwords shall be a minimum of 8 characters.
    C. Passwords shall be a mixture of letters (upper and lowercase), numbers, and special characters (for example: !, @, #, $, %).
    D. Passwords shall be kept secret and secure and shall not be disclosed to anyone else for any reason.
    E. Passwords shall not be written down.
    F. All account Passwords shall be changed on a regular basis (no more often than every 90 days).
    G. The Company will set and periodically update all default passwords (or establish passwords where not preset) for network resources (e.g., routers, wireless networks).

d. User Account Administration, Permissions Management, and Password Management

i. Rights and responsibilities for creating user accounts and establishing passwords shall be vested in one or a few key employees and controlled closely.
ii. All system account passwords shall be documented. These accounts are typically used for inter-process communication and frequently cannot be changed on a regular basis. The permissions associated with these accounts shall be kept as narrow as possible.

iii. Software systems shall be configured to use Windows authentication or, alternatively, programmatically meet the equivalent of these password recommendations.
iv. Single sign-on schemes shall be used, where available, to establish a single user identity for multiple systems and/or applications.
v. Specified procedures shall be followed to ensure that employees have the proper access upon hire, upon any job changes, and are removed from the system after termination of employment.
vi. Separate accounts and passwords shall be established for each individual user. User accounts shall not be shared among multiple employees. Office-wide passwords or shared codes shall not be used.
vii. Permissions features for software applications shall be used to manage access to technology, limiting NPI access to appropriate employees.
viii. Permissions and rights features for network and storage devices shall be used to limit access to employees with express authorization and legitimate business purpose for access to the NPI (e.g., to carry out job duties).

e. Data accessed remotely or stored on mobile devices

Mobile devices will be subject to the following Company controls:

It is the responsibility of any employee of Independence Title who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct Independence Title business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

i. Company reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. Company's IT staff will engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users and clients at risk.

ii. Prior to initial use on the corporate network or related infrastructure, all mobile devices must be approved by Company**.**

iii. All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by Independence Title's IT department. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect.

iv. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

v. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This practice includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by Independence Title's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

vi. Passwords and other confidential data as defined by Independence Title's IT department are not to be stored unencrypted on mobile devices.

vii. Any mobile device that is being used to store Independence Title data must adhere to the authentication requirements of Independence Title's IT department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by Independence Title's IT department before any enterprise data-carrying device can be connected to it.

viii. IT will manage security policies, network, application and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Company's security policy.

ix. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required. Detailed data wipe procedures for mobile devices will be provided.

x. In the event of a lost or stolen mobile device it is incumbent on the user to report the loss or theft to Company IT staff immediately. The device may be remotely wiped of all data and locked to prevent access by unauthorized parties.

xi. Independence Title's IT department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware or software. This applies even to devices already known to the IT department.

xii. Employees, contractors and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of Independence Title's IT department. This includes, but is not limited to, any reconfiguration of a mobile device.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

xiii. Company reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

xiv. Company may establish audit trails, and these may be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to Company's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Company's highest priority.

xv. The end user agrees to immediately report to his/her manager and Company's IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

xvi. Employees will not be granted mobile device access to Company resources unless they have reviewed and accepted the mobile device policy.

f. Collection and Transmission of Non-public Personal Information Shall Be Secure and/or Encrypted

i. The Company will not store data, files, or other information stored on computer servers, desktops, copiers, laptops, smart phones, tablet computers, removable storage devices, etc. in an unencrypted storage location (not a desktop/workstation) or on encrypted portable devices and electronic media. These types of data should be stored on the Company network.

ii. Employees should never load database files or applications, such as title production software, on personal computers.

iii. Employees should never store NPI on personally owned devices.

iv. Employees will delete files from portable devices and electronic media when they are no longer needed.

v. The Company will physically secure assets with NPI by securing physical access to the server room and/or server hardware.

vi. The Company will password-protect all Company owned laptop computers, portable devices, and electronic media containing NPI.

When data including data files, documents or other communications containing NPI are sent or received over a network or from one device/user to another device/user, the following practices will be used:

vii. Email, both inbound and outbound, shall be reviewed to determine if data containing NPI is being sent un-encrypted from the Company or received by the Company. If email containing un-encrypted NPI is being received (e.g., closing packages from lenders, preliminary HUD-1 statements), the Company should proactively contact the sender to request an alternative delivery method.

A. Protect email content:

1) The Company shall establish and own its own true business domain (@Company.com), email server and address.
2) The Company shall not use any public and/or free email addresses like gmail.com, aol.com, hotmail.com, etc.
3) For transmission of NPI in the subject of, body of or attachment to the email, Company shall use an email encryption service.
4) Spam or content filtering shall be used on email servers.

g. Portable Media

Examples of portable physical media include, but are not limited to: laptops, USB drives, CDs, DVDs, tapes and flash drives. The

loss or theft of a laptop or other supported media device must be reported immediately to the Company's administrative staff.

i. Portable devices, data, and files containing NPI shall be password-protected or encrypted.
ii. Portable devices, data and files containing NPI shall not be left in an unlocked vehicle or a location visible from outside the vehicle.
iii. Portable devices, data and files containing NPI shall not be left unattended in a hotel room, conference room, reception area or any other location that can be accessed by others.
iv. Each user is responsible to protect portable devices containing NPI in their possession from theft or unauthorized access.

h. Network Vulnerability Testing

Network vulnerability testing shall be performed periodically to ensure that NPI and the Company network are protected. Testing shall be performed with reasonable frequency and the results of such tests shall be documented and kept on file. Remediation of any discovered vulnerability shall be initiated with reasonable promptness under the circumstances, taking into consideration the severity of the vulnerability uncovered.

8. Backup Policy and Procedures

The Company requires that computer server systems be backed up periodically and that the backup media is stored in a secure off-site location. The purpose of the systems backup is to provide a means to: (1) restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, and (2) provide a measure of protection against human error or the inadvertent deletion of important files. The systems backups will consist of regular full and incremental backups and will be stored in a secure off-site location based on the schedule listed below.

a. Back-Up Procedures

Company's servers are backed up at time frames appropriate to the data and processes they support.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

b. Storage of Back-Ups

All weekly, monthly or annual backups will be stored in a secure, off-site location. If a tape is used, then proper environment controls, including temperature, humidity and fire protection shall be maintained at the storage location.

c. Storage of Back-Ups

All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.

d. Testing of Back-Ups

Periodic tests of the backups will be performed by the Company IT department to determine viability.

9. Retention and Destruction of Non-public Personal Information

a. All physical media containing NPI shall be protected from unauthorized disclosure, modification, removal, and destruction**.** The Company shall implement additional procedures as necessary to protect against unauthorized access to or use of data in connection with its disposal. Application of such measures may depend on a number of factors, including the sensitivity of the information, costs and benefits of different disposal methods, available technology, and applicable legal requirements.

b. Before disposing of hardware (*e.g.*, copies, computers and other electronic devices) and physical media, the Company shall encrypt decommissioned hardware components which may have files containing NPI (servers, computers, laptops, copiers, scanners, fax machines, backup tapes rotated out of use, etc.) before deleting data and/or destruction. Alternatively, hard drives may be shredded or taken to an approved electronics disposal provider. All NPI stored therein must be removed or made unrecoverable. If the NPI cannot

be made unrecoverable, physical destruction of the hardware or physical media is required.

c. This requirement also applies to equipment which is leased or rented; therefore, the Company reviews all lease agreements to determine if disposal policies are consistent with the protection of NPI.

d. The Company shall maintain locked shredding containers for documents containing NPI that are to be destroyed periodically.

10. Overseeing Third Party Service Providers

a. The Company shall conduct reasonable due diligence on all third party service providers prior to hiring each service provider.

b. The Company's administrative staff shall develop and incorporate standard, contractual protections applicable to third party service providers and its subcontractors, which will require the service provider (and its subcontractors) to implement and maintain appropriate information security safeguards for NPI**.** When entering into contracts with third party service providers which affect NPI, the Company will obtain certain written assurances (either in the services agreement or a standalone confidentiality agreement) from each third party provider regarding its handling of NPI. At a minimum, these written assurances shall provide that the service provider (and subcontractors, if applicable) shall:

i. Provide evidence reasonably satisfactory to allow the Company to confirm that such party has satisfied its obligations regarding the handling of NPI.

ii. Provide immediate notification to the Company following discovery of any breach or suspected breach involving NPI.

iii. To the extent the service provider is unwilling to include such language in the contract or in a separate acknowledgment, the Company will seek to obtain an alternative form of assurance.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

c. Fee Attorney Offices

i. Company will obtain a signed Confidentiality Agreement from each attorney Fee Office before the Fee Office becomes a transactional agent of Company, or as soon as practically possible from each existing Fee Office after this Best Practice is put into effect. The Confidentiality Agreement may be made an addendum to the Fee Office's existing fee attorney agreement with the Company.

ii. The Confidentiality Agreement will reflect, among other things, that:

A. Any NPI that the Fee Office comes into contact with while transacting business for Company must be protected according to the standards contained in this Policy;

B. The Fee Office must not share the NPI with third-party service providers, unless acknowledged by both parties in the Agreement;

C. Any NPI that Fee Office still has in its possession at the termination of business and agency with Company must be turned over to Company immediately.

11. Data Breach Incident Reporting

The Company shall take all necessary actions to protect NPI in accordance with this Privacy Program and applicable legal requirements. Actual and suspected data breach incidents shall be reported, investigated, and handled in a timely manner. The Company shall work with the affected clients and consumers and local law enforcement as may be appropriate in the circumstances.

12. Business Continuity and Disaster Recovery

Business continuity and disaster recovery planning shall be an integral part of information systems security to ensure timely resumption from and, if possible, prevention of interruptions to business activities and processes caused by failures of information systems. The Company shall take appropriate measures to protect facilities and equipment from physical and environmental threats to prevent loss, damage, theft, or compromise of assets and interruption to business activities.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

13. Enforcement

Noncompliance with this Best Practice Policy, whether intentional or negligent, may result in discipline up to and including immediate termination of employment. The Company will determine appropriate disciplinary actions under the circumstances and in accordance with applicable Company policies and local, state, and federal law. The Company's administrative staff may establish procedures for obtaining exceptions from the requirements of this Program under appropriate circumstances.

Employees who violate this Privacy Program may be held personally responsible for any damages caused by loss of NPI resulting from their actions. Where a violation of this Privacy Program also constitutes a violation of state or federal law, the Company may report such actions to the appropriate federal and state law enforcement authorities.

14. Program Revision History

The Company's administrative staff will review this Policy at least annually and make any updated needed to reflect changes in operations, legal and regulatory requirements, industry best practices, and available technology.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

REAL ESTATE SETTLEMENT PROCEDURES

Best Practice No. 4: Adopt standard real estate settlement procedures and policies that help ensure compliance with Federal and State Consumer Financial Laws as applicable to the settlement process.

Purpose: Adopting appropriate policies and conducting ongoing employee training helps ensure the Company can meet state, federal, and contractual obligations governing the settlement (hereinafter, "closing").

Company Policies and Procedures for Implementation and Adherence to Best Practice No. 4:

1. Recording Procedures

The Company:

a. Reviews legal and contractual requirements to determine Company obligations to record documents and incorporate such requirements in its written procedures.

b. Electronically submits or ships documents for recording to the county recorder (or equivalent) or the person or entity responsible for recording within two (2) business days of the later of (i) the date of closing, or (ii) receipt of documents by the Company if the closing is not performed by the Company.

c. Tracks shipments of documents for recording.

d. Ensures timely responses to recording rejections.

e. Addresses rejected recordings to prevent unnecessary delay.

f. Verifies that recordation actually occurred and maintains a record of the recording information for the document(s).

2. Pricing Procedures

The Company:

a. Maintains written procedures to ensure customers are charged the correct title insurance premium and other rates for services provided by the Company. These premiums and rates are determined by a mix of legal and contractual obligations.

b. Utilizes rate manuals and online calculators, as appropriate, to help ensure correct fees are being charged for title insurance policy premiums, state-specific fees and endorsements.

c. Ensures discounted rates are calculated and charged when appropriate, including refinance and reissue rates.

d. Performs quality checks after closing to ensure consumers were charged promulgated policy premium rates.

e. Provides timely refunds to consumers when an overpayment is detected.

3. Payoff Information

The Company shall obtain a payoff statement good through closing for any and all existing mortgages or deeds of trust to be satisfied in the transaction and shall seek authority as appropriate to obtain such payoff statements.

4. Review the Sales Contract

The Company shall review the sales contract, if any, and advise consumers on any changes that may be necessary for Company's escrow or title insurance purposes for the specific transaction.

5. Supervise Execution

At the closing of each transaction occurring at a Company office, a Company escrow officer shall supervise the proper execution and notarization of the closing documents that are signed at the closing table.

6. Collection of Funds

At the closing, a Company escrow officer shall collect funds required to close from the respective parties and verify that closing funds are good funds in accordance with the applicable law and/or regulation and any other internal bank regulations.

7. Funding Approval

Following the closing and prior to recordation, a Company escrow officer or escrow assistant shall forward all required funding documents to Lender for Lender's funding approval and shall obtain Lender's funding approval prior to recording.

8. Perform Title Update

Prior to the closing conference and prior to recordation, but in any event, not later than at such time as is concurrent with presenting the documents for recording, a Company title officer or title examiner shall update or supervise performance of title update prior to recording to verify no intervening matters (liens, judgments, conveyances, etc.) appear of record since the last Title Insurance Commitment effective date.

9. Recording

    a. Local Physical Recordation

        After the closing, and within one business day following closing, Company's escrow team shall record or supervise the recording of the recordable closing documents in the proper order.

b. Remote Physical Recordation

If the documents are to be physically presented at a remote location for recordation, then following the closing and within two business days, a Company escrow team shall dispatch the documents to the appropriate county clerk's office with a receipt required overnight delivery service and present for recording the recordable closing documents in the proper order.

c. Electronic Recordation

If the documents are to be electronically filed, following the closing and within 24 hours of Settlement, a Company escrow team shall electronically present the recordable documents for recording in the proper order.

10. Disbursement

A Company escrow officer shall disburse all of the closing funds in accordance with the Combined Disclosure Statement and lender's closing instructions after confirmation of recording**.** If any funds were collected in excess of what was actually disbursed, a refund to the consumer or appropriate party should be issued immediately.

11. Notice of Recording to Parties

Recorded instruments from each transaction shall be returned to the parties by the Company as appropriate.

TITLE POLICY PRODUCTION

Best Practice No. 5: Adopt and maintain written procedures related to title policy production, delivery, reporting and premium remittance.

Purpose: Adopting appropriate procedures for the production, delivery, and remittance of title insurance policies helps ensure title companies can meet their legal and contractual obligations.

Company Policies and Procedures for Implementation and Adherence to Best Practice No. 5:

1. Collection of Information and Review

    a. Intake of Title Request

    Upon receipt of a Title Request:

    i. a guaranty file shall be opened,

    ii. the receipt of the title request shall be acknowledged by the Company, and

    iii. the Company shall initiate preparation of a title insurance commitment.

    b. Investigate Title

A Company title examiner shall perform or supervise a detailed title search of the subject property and the examiner or a Company title officer shall personally review the title abstract, notes and title documents prior to personally preparing an examiner's report and commitment for title insurance, noting any curative measures that must be completed prior to closing.

The general steps of the title search should include, but are not limited to, the following:

Review of an abstract of title reflecting instruments in the chain of title for the subject property found of record in the public records of the local county,

including real property records, district court records, and probate court records, and examination of such recorded instruments as are revealed by the abstract of title. The examiner or title office shall also perform a eview of known bankruptcy information affecting the subject property.

c. Legal Description

A Company title examiner shall review the legal description of the subject property, noting any inconsistencies in prior deeds or the contract, as well as taking any curative measures that must be completed prior to closing.

d. Covenants, Conditions, and Restrictions (CCRs)

A Company title examiner shall disclose on the title insurance commitment the existence of any covenants, conditions, and restrictions (CCRs) that run with the land and affect title insurance coverage for the land by making appropriate exception for such CCRs in the title insurance commitment.

e. Review Title Commitment

A Company title officer, in tandem with a Company escrow team, shall where circumstances demand, review title insurance company's commitment for title insurance and verify compliance with the requirements and exceptions of that commitment, and obtain, prepare, review, and/or provide any documents required by the title insurance company to issue a final title policy.

2. Verification and Final Title Review

a) Cancellations of Liens, Judgments, and Deeds of Trust

i. If included within the scope of the transaction closing, a Company escrow officer shall obtain cancellation(s)/satisfaction(s) of record of any lien(s), judgment(s), and/or deed(s) of trust paid off and released as a result of the transaction.

b) Perform a Final Title Review
Following the closing, a Company policy team shall review the final title and recording information.

3. Policy Issuance

Title insurance policies are Issued and delivered to customers within thirty (30) days of the later of (i) the date of closing, or (ii) the date that the terms and conditions of the title insurance commitment are satisfied.

4. Underwriter Reports and Remittance

By the last day of the month following the month in which an insured transaction was settled, the Company:

a. Reports to the title insurance underwriter all of the policies issued during the current month.

b. Remits to the title insurance underwriter all of the premiums and fees collected and due to the title underwriter.

PROFESSIONAL LIABILTY INSURANCE

Best Practice No. 6: Maintain appropriate professional liability insurance and fidelity coverage.

Purpose: Appropriate levels of professional liability insurance or errors and omissions insurance help ensure title agencies and settlement companies maintain the financial capacity to stand behind their professional services. In addition, state law and title insurance underwriting agreements may require the Company to maintain professional liability insurance or errors and omissions insurance, fidelity coverage or surety bonds.

Company Policies and Procedures for Implementation and Adherence to Practice No. 6:

The Company maintains and shall continuously maintain professional liability insurance or errors and omissions insurance in an appropriate amount given the Company's size and complexity, and the nature and scope of its operations. The amount is not less than the amount agreed to in the Company's contractual obligations to its underwriters and state law, if applicable. This includes but is not limited to:

1. Professional liability or errors and omissions insurance

    a. The Company maintains professional liability insurance in the amount of no less than $1,000,000.00. This amount is appropriate given the Company's size and complexity and the nature and scope of its operations; the amount is not less than the amount agreed to in the Company's underwriting agreement(s).

    b. The insurance carrier is nationally known and has appropriate Best ratings.

    c. Coverages / endorsements are reviewed annually and are added or subtracted to reflect current changes in the practices of the industry and to reflect new threats to our business as they arise, such as cybercrime.

2. Fidelity bond coverage

The Company maintains a fidelity bond policy in an amount of not less than $550,000.00. The company reviews both state law and its Issuing Agency Contracts to verify that Company coverage meets or exceeds their respective requirements. This coverage is carried even if state law or Company's Issuing Agency Contract does not require it from time-to-time as conditions or laws change.

3. Surety coverage, Closing Protection Letters

Company offers insured closing letters through its title insurance underwriters in accordance with state regulation.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.

ADDRESS CONSUMER COMPLAINTS

Best Practice No. 7: Adopt and maintain written procedures for resolving consumer complaints.

Purpose: A process for receiving and addressing consumer complaints helps ensure reported instances of poor service or non-compliance do not go undiscovered.

Company Policies and Procedures for Implementation and Adherence to Best Practice No. 7:

The Company shall maintain written procedures for resolving consumer complaints, which includes a standard complaint form, suitable point(s) of contact, and procedures for logging and resolution of complaints. The log of consumer complaints will include whether and how the complaint was resolved.

1. Consumer Complaint Contact and Responsibilities

    a. The Company will establish suitable complaint contact(s). A complaint contact is responsible for:
        i. Ensuring that consumer complaints are timely addressed;
        ii. Administering and maintaining the consumer complaint log;
        iii. Administering and maintaining the consumer complaint files in an orderly and professional manner, including but not limited to:
            A. Any consumer complaint forms
            B. All correspondence related to the consumer complaint; and
            C. All supporting documentation related to the consumer complaint.
        iv. Investigating the nature and credibility of the consumer complaint, including but not limited to:
            A. Investigation of the consumer complaint;
            B. Making a determination as to the validity and credibility of the consumer complaint;

C. Making a determination as to the person or persons (inside or outside the Company) that is or are responsible for the facts and circumstances that led to the consumer complaint;
D. Making a determination as to the best possible resolution for the consumer complaint; and
E. Pursuing the best possible resolution for the consumer complaint; and
F. Informing the senior executives and principals of the Company of the status of filed, resolved and unresolved complaints on at least a monthly basis.

2. Consumer Complaint Intake

a. Every employee is informed and aware that consumer complaints may come to the Company in many forms, including but not limited to,:
    i. Phone Calls
    ii. Letters (Regular Mail)
    iii. Certified Mail
    iv. Facsimile
    v. Emails
    vi. Voice Mail
    vii. Legal Action
    viii. Company Website
b. Any employee who receives a consumer complaint from a customer has a duty to pass that information on to the complaint contact(s), so that the log of complaints is accurate and up-to-date.
c. All complaints that are reasonably likely to produce a formal consumer complaint, and all complaints that actually result in formal consumer complaints shall be detailed by the employee who received the complaint information in the appropriate format and sent timely to the complaint contact(s) for review.

3. Consumer Complaint Policy

While not every cause for consumer complaint is due to Company's error, the Company remains dedicated to pursuing a resolution for each consumer complaint that is preferable and acceptable to the consumer and the Company.

Independence Title Company reserves the right to modify these Best Practice policies at any time. However, as of the date presented, this statement reflects the presently adopted Best Practice policies of Independence Title Company.