Written Information Security Program

Effective: June 2024

Policy Statement
The Midland Title and Escrow, Ltd. (Company) Written Information Security Program (WISP) is intended as a set of comprehensive guidelines and policies designed to safeguard all Non-public Personal Information maintained by the Company, and to comply with applicable laws and regulations regarding the protection of Non-public Personal Information, as that term is defined below, found in records and in systems owned and/or maintained by the Company.

I. Objective

The objective in developing and implementing this comprehensive WISP is to create effective administrative, technical and physical safeguards that are appropriate to the size, scope and type of business of the Company, the amount of resources available to the Company, the amount of Non-public Personal Information (NPI) stored (electronically and physically), and the need for security and confidentiality of both consumer and employee information. This WISP sets forth the Company's procedures for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting consumers' and employees' NPI.

For purposes of this WISP, "Non-public Personal Information" means an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual:

a. Social Security number;

b. driver's license number or state-issued identification card number; or

c. financial account number, or credit or debit card number, with any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; or

d. a user name or e-mail address, in combination with a password or security question and answer, that would permit access to an online account; or

e. Biometric records; or

f. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

Provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

II. Purpose & Scope

The purpose of this WISP is to:

- ensure the security and confidentiality of employee and consumer NPI;
- protect against any anticipated threats or hazards to the security or integrity of such information; and
- protect against the unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

In formulating and implementing this WISP, the Company has identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing NPI. The Company has also assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information. In addition, the Company has evaluated the sufficiency of existing policies, procedures, customer information (company and document management) systems, and other safeguards in place to control such risks.

This WISP has been designed and implemented to put safeguards in place to minimize identified risks, consistent with all applicable state and/or federal requirements; and to regularly monitor the effectiveness of those safeguards.

III. Security Manager

The Company has a designated Security Manager who will be responsible for the following:

a. Implementation of the WISP.

b. Maintaining and updating the WISP at least annually (in accordance with e. and f. below).

c. Training Company owners, employees, both temporary and permanent, through initial as well as ongoing training, on the WISP, the importance of maintaining the security measures set forth in this WISP, and the consequences of failures to comply with the WISP.

d. Assessing employees' compliance with the measures of the WISP.

e. Reviewing the scope of the security measures set forth in the WISP at least annually, or whenever there is a change in business practices that may implicate the security or integrity of records containing NPI, and modifying the WISP accordingly.

f. Monitoring the effectiveness of the security program set forth in the WISP, testing the safeguards contained therein, and making changes to the WISP when necessary.

g. Evaluating third-party providers' contracts and agreements to ensure providers can meet the NPI protection standards and requirements contained in this WISP.

IV. Risks

The following areas have been identified as reasonably foreseeable internal and external risks and have been assessed, considering the safeguards which are implemented as part of this WISP, as noted:

1. Non-public Personal Information is used during the preparation of real estate closing documents.

    - Some of this NPI is found on paper records and files that are maintained at employees' desks while the corresponding transactions are active. Some additional paper files and documents containing NPI are kept in a locked filing cabinet.

    - Upon completion of a transaction, the paper records and files for Residential transactions are shredded and/or placed in a locked shred bin until a third-party service provider, AccuShred, is called to collect and dispose of these papers via shredding. Paper records and files for Commercial transactions are stored in a locked file area in the basement of the Downtown office. A key is required to access these files. Only designated employees in the title department have access to the key.

    - NPI is also maintained in an electronic format within Company systems, which contain both client and employee NPI. All Company employees have a unique user ID and password for systems that contain NPI, and security permissions are set to restrict access to employee data to management only.

2. Authorized Company employees have physical access to the locked filing cabinets that are maintained at the Company that contain NPI. These Company employees are deemed to have a true, business-related need, to have access to said information.

3. NPI is also transmitted digitally, including via email, during the course of normal Company operations. All digital transmission of NPI is encrypted to render the personal information unreadable and/or unusable.

V. Safeguards

The measures in this section are now implemented to address the risk areas noted in the above section of the WISP.

A. Safeguards Against Internal Risks and Threats

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing NPI, and to evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

1. An electronic copy of the WISP will be distributed to each employee, and new employees, who shall, upon receipt of the WISP, acknowledge that he/she has received a copy of the WISP.

2. The Company utilizes Corporate Intelligence Consultants as the information provider for background and credit checks. The Company individuals who have access to NPI is restricted to authorized principals and employees who have undergone a formal background check and credit report process which identified no irregularities.

3. There will be immediate training and annual retraining of employees on the detailed provisions of the WISP.

4. All employees are required to comply with the provisions of this WISP and are prohibited from using NPI in any nonconforming manner during or after employment. Disciplinary action will be imposed for violations of the security provisions of this WISP, taking into account the nature of the violation and the nature of the NPI affected by the violation. A portion of employees' performance evaluations will be based on the adherence to the provisions of this WISP.

5. The amount of personal information collected should be limited to that amount reasonably necessary to accomplish the Company's legitimate business purposes, or necessary for the Company to comply with other state or federal regulations. The NPI required for the Company's legitimate business purposes includes, but is not limited to, consumers' names, addresses, social security numbers, and drivers' license numbers.

6. Access to records containing NPI shall be limited to those persons who are reasonably required to access such information in order to accomplish the Company's legitimate business purpose or to enable the Company to comply with other state or federal regulations.

7. Electronic access to user identification shall be blocked after multiple unsuccessful attempts to gain access. The IT service provider shall be responsible to determining the number of unsuccessful attempts that will be permitted prior to blocking access.

8. Employees are prohibited from removing files, records or documents that contain NPI from the Company's premises overnight. NPI may only be removed from the offices in approved instances, including remote closing and transport of paper files between company offices.

9. All security measures shall be reviewed at least annually, or whenever there is a material change in the Company's business practices that may reasonably implicate the security or integrity of records containing personal information. The Security Manager shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.

10. Terminated employees shall return all records containing NPI, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).

11. An employee's physical and electronic access to NPI shall be immediately blocked upon termination. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or information. Moreover, such terminated employee's remote electronic access to NPI must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

12. Current employees' passwords used to access Company systems must be changed periodically and must meet minimum complexity requirements. Currently the policy requires passwords to be changed every 30 days and minimum password length is 12 characters. All The Company's computers no mater, desktop or laptop run a "screen timeout" application causing automatic system sign off when the system detects no activity for a period of 5 minutes.

13. At the direction of Donald M Mewhort III President, The Company's designated Network Administrator grants appropriate access to The Company's various computer technology applications. The Company's file server(s) or main central processing unit is housed off sight in a highly secured environment. The Company's computer network utilizes up-to-date anti-virus, anti-spyware and data encryption software applications. The Network Administrator is responsible for such software maintenance.

14. Access to personal information shall be restricted to active users and active user accounts only.

15. Employees are required to report any suspicious or unauthorized use of NPI to their supervisor.

16. Whenever there is an incident that requires notification under any applicable state and/or federal laws, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in the Company's security practices are required to improve the security of NPI for which the Company is responsible.

17. Employees are prohibited from keeping open files or documentation containing NPI on their desks when they are not at their desks. Employees shall use a locked drawer to store documentation that contains NPI while away from their desks.

18. The Company has developed the following rules that ensure reasonable restrictions upon physical access to records containing NPI are in place.

    a. Any documentation or files containing NPI are to be stored in a locked room when employees leave for the day.

    b. Visitors' access is restricted to the front door of the Company, and visitors shall not be permitted to visit unescorted any area within Company premises that contains NPI.

c. While visitors (clients or prospects) are at an employee's desk, any files or documentation containing NPI shall be maintained out of the sight of the visitor(s), unless the documentation or files pertain to said visitor.

19. Access to electronically-stored NPI shall be limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for a period of time as determined by the Security Manager.

20. Paper or electronic records (including records stored on hard drives or other electronic media) containing NPI shall be disposed of only in a secure manner in compliance with any applicable state and/or federal requirements. All paper records and files (after scanning if appropriate), after being processed in accordance with Company protocol, will be shredded and/or placed in the locked shred bin. The Security Manager will maintain the key and lock for the shred bin and will be responsible for contacting the shredding company to dispose of the paper files as needed.

B. Safeguards Against External Risks and Threats

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information, and to evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are currently in place:

1. Firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, are installed on all Company systems processing and/or storing NPI. These protections are updated daily automatically (and manually when needed) on all Company systems.

2. System security software, which includes malware protection, patches and virus definitions, is installed on all Company systems processing and/or storing NPI. This software is updated daily automatically (and manually when needed) on all Company systems.

3. All records and files transmitted across public networks, e.g., via email or wirelessly, must also be, to the extent technically feasible, encrypted. Encryption requires the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key, unless otherwise defined by applicable state and/or federal requirement.

4. Any portable electronic device or laptop that is used in Company operations or that contains NPI for Company clients, prospects, or employees must also be encrypted as defined in the above paragraph. There will be no laptops used for company business which are not previous encrypted by CISP, IT service provider.

5. All Company computer systems will be monitored for unauthorized use of or access to personal information. Any unauthorized use or access found will be immediately reported to the Security Manager. In addition, action will be taken to assess the impact of the unauthorized use/access, appropriate measures will be taken against employees

not complying with this WISP, and updates will be made to the safeguards specified in this WISP if needed to prevent future unauthorized access/use of NPI.

6. Secure user authentication protocols are in place on Company systems, including (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords; (3) control of data security passwords to ensure that such passwords are kept in a secure location (e.g., a password manager).

7. CISP performs daily backups of Company data. Backups are offline and disconnected with Midland's network or stored with a could provider with MFA access secured. Backups are managed by CISP, IT service provider.

8. The Company only partners with third parties which are able to provide SOC 2 reports supporting their security controls. SOC 2 reports and Privacy Policies are reviewed by management during the vetting process. All third parties must also be approved on the FNF Solution Partners to ensure they meet appropriate criteria for industry standards.