TDI TITLE DATA
Excellence by Design

Texas Based. Texas Strong.

1225 North Loop West, Suite 950
Houston, Texas 77008
713.880.2600 | www.titledata.com

NPPI Privacy and Security Policy

Statement of Purpose

This NPPI Privacy and Security Policy ("Policy") sets forth the privacy and security practices of Title Data, Inc. and its subsidiaries (collectively "TDI") with respect to Non-public Personal Information (NPPI). It is the policy of TDI to protect the confidential nature of NPPI.

Types of NPPI TDI Collects

- **Password holders:** TDI collects information that can be used to distinguish a prospective computer password holder and current computer password holders (collectively a "password holder") from a non-password holder and includes name, home address, personal telephone number, last 4-digits of the Social Security Number and date of birth.

- **Title orders stored in a title plant:** Customers entrust TDI with information which pertains to a pending real estate transaction when the customer opens a title order in one of TDI's title plants; such information may include the names of the parties to the pending real estate transaction and the fact that a real estate transaction is pending for a specific parcel of real property.

- **Digital starters received from a customer:** Customers entrust TDI with digital copies of title insurance commitments which may include the name or names of the proposed insured and the proposed policy amount or amounts.

Use of NPPI: Password Holders

TDI does not sell any NPPI collected from password holders and, except as set forth below, TDI does not release such NPPI to third parties. NPPI collected by TDI in the course of reviewing a computer password request, issuing a computer password or changing a computer password may be used for the following purposes:

- To check the background of a prospective password holder

- To distinguish a password holder from all other password holders

- To create a password holder's User Profile and User ID

- To investigate possible unauthorized use of TDI's trade secret records and information

Use of NPPI: Title Orders; Digital Starters

TDI does not sell or disclose to unauthorized third parties NPPI which pertains to a pending or closed title order. TDI only discloses digital starters to customers who are contractually bound to use such digital starters for the limited purpose of preparing and issuing a promulgated title insurance product pursuant to a bona fide real estate transaction pertaining to the parcel of real property which is the subject of the digital starter.

Security for NPPI

The security of NPPI is very important to TDI. TDI maintains physical, electronic, and procedural safeguards to protect the confidentiality of NPPI, including:

- **Storage of physical documents containing NPPI:** Hardcopy documents containing NPPI are stored in a locked vault monitored 24x7 by a video-surveillance system; no documents containing NPPI are left unsecured, either during or after the work day (our "clean desk" policy).

- **Access by TDI employees:** Documents containing NPPI, whether such documents be in hardcopy or electronic form, are accessible by a limited number of TDI's bona fide employees [who underwent background checks at hiring] and then only for the legitimate business purposes set forth above.

- **Web services:** All TDI web services requiring password authentication utilize SSL certificates issued by a third party for encryption purposes.

- **Network connections:** Network connections created by a TDI customer to connect to TDI require the use of a VPN IPSec/SSL connection. These customer VPN connections terminate to a secure DMZ-zone network which is separate and apart from TDI's internal private network, and TDI incorporates Access Control Lists (ACLs) to prevent unauthorized access.

- **Network security:** TDI does not permit direct access to a title plant's server or associated image library; access is solely by means of TDI's TIMS® client application using password authentication. All NPPI is secured behind redundant firewalls in a DMZ network, accessible only via a TDI-authorized VPN connection; NPPI is *never* stored in a publicly accessible server or an employee-owned device.

- **Password management:** Passwords are controlled by TDI via one-way encryption [hash] and users are required to change passwords periodically [previously used passwords cannot be reused].

- **Physical security:** TDI's network resources are physically located in secure, restricted-access space monitored 24x7 by a video-surveillance system; all access to this space is logged and requires an access code. Additionally, this restricted-access space is located in a building which employs on-site 24x7 security.

- **Data protection:** TDI replicates data to a professionally managed disaster recovery site, and system back-ups utilize encryption. Other than for back-up purposes, NPPI is not stored on removable devices, including without limitation laptops, tablets, smart phones, USB drives and similar.

- **FTP protection:** TDI supports SSL SFTP Public Key Authentication for the transmission and receipt of data to and from remote locations. SSL SFTP provides encryption and requires both a public and private SSL key.

- **Disaster recovery plan and testing:** TDI updates its disaster recovery plan quarterly and conducts a live roll-over to its disaster recovery site at least once a quarter.

Disposal of NPPI

Hardcopy documents containing NPPI are shredded prior to disposal. Electronic records containing NPPI which are stored (i) in a computer's memory or disk are destroyed prior to disposal of such memory or disk, and (ii) in back-up media (such as magnetic tapes, CDs and DVDs) are rendered unviewable and unusable during the physical destruction process TDI employs prior to disposal.

Questions; Reporting Breaches

If you have questions or concerns about this Policy or wish to report a known or suspected breach of TDI's security measures, please contact us at kgugenheim@titledata.com.