



## **Privacy Policy**

### **Statement of Purpose**

This Privacy Policy (“Policy”) sets forth the privacy practices of Title Data, Inc. and its subsidiaries (collectively “TDI”) with respect to personally identifiable information collected from prospective computer password holders and current computer password holders (collectively a “password holder”). “Personally Identifiable Information” means information that could be used to name or distinguish a password holder from a non-password holder and includes, without limitation, name, home address, home telephone number, Social Security Number, date of birth, and driver’s license number. It is the policy of TDI to protect the confidential nature of Personally Identifiable Information. Therefore, in order to protect and maintain the confidentiality of such information, TDI has enacted this Policy.

### **Use of Personally Identifiable Information**

Personally Identifiable Information collected by TDI in the course of reviewing a computer password request, issuing a computer password or changing a computer password will be used for the following purposes:

- To check the credit and criminal background of a 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

### **Release of Personally Identifiable Information**

TDI does not sell any Personally Identifiable Information. Except in the investigation of possible unauthorized use of TDI’s trade secret records and information, TDI does not release any Personally Identifiable Information to third parties, and then only as required by (i) investigators and attorneys retained by TDI and/or (ii) law enforcement officials and judicial authorities. TDI reserves the right to report to law enforcement agencies any activities that TDI in good faith believes to be unlawful.

### **Security for Personally Identifiable Information**

The security of Personally Identifiable Information is very important to TDI. TDI restricts access to Personally Identifiable Information to those TDI employees which have a legitimate business purpose to view and use Personally Identifiable Information. TDI maintains physical, electronic, and procedural safeguards to protect the confidentiality of Personally Identifiable Information, including:

- Documents containing Personally Identifiable Information, whether such documents be in hardcopy or electronic form, are accessible by a limited number of TDI's bona fide employees and then only for the purposes set forth above.
- Personally Identifiable Information incorporated into a User ID or entered by a password holder is secured by (i) 3DES 168-bit encryption (for transmissions between a password holder's personal computer and TDI's servers when the password holder is connected to TDI by TDI's virtual private network), and (ii) features and functionality inherent to a dedicated communications network when password holders are connected to TDI by means of TDI's dedicated communications network.
- Personally Identifiable Information is never stored in a publicly accessible computer.

### **Disposal of Personally Identifiable Information**

Hardcopy documents containing Personally Identifiable Information are shredded prior to disposal. Electronic records containing Personally Identifiable Information which are stored (i) in a computer's memory or disk are deleted 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.

### **Contact Information**

If you have questions or concerns about this Policy please contact us at [jsibley@titledata.com](mailto:jsibley@titledata.com).