

Knight-Barry Title Group GLBA Security Policy

INTRODUCTION, PURPOSE AND SCOPE

The Graham Leach Bliley Act (“GLBA”) requires financial institutions to protect non-public information from being disseminated beyond the control of the financial institution’s network. The Knight-Barry Title Group (“KBTG”) is comprised of Knight-Barry Title, Inc., Port Abstract & Title LLC, and Knight-Barry Title Services LLC (“collectively “KBTG”). Because KBTG provides services to financial institutions subject to GLBA, and receives non-public information from customers of financial institutions for use in KBTG’s title insurance, title reports, loan closings and related services (collectively “Products and Services”), KBTG complies with GLBA. KBTG has established the safeguards contained in this policy under the following categories:

- I. Types of non-public information contained in our Products and Services.
- II. Criteria for identifying information subject to this policy.
- III. Roles and Responsibilities
- IV. General Physical Security Measures
- V. General Technical Security Measures
- VI. Auditing
- VII. Summary

I. TYPES OF NON-PUBLIC INFORMATION

KBTG’s Products and Services are comprised of a search of the public record as a service to financial Institutions. As such, we are regularly compiling documents from the public record which may contain non-public information such as social security numbers. In addition, financial institutions furnish KBTG with non-public information in the form of social security numbers, savings and checking account numbers, etc, contained in loan application and loan closing documents.

II. CRITERIA FOR IDENTIFYING INFORMATION SUBJECT TO THIS POLICY

KBTG periodically evaluates information contained in its Products and Services against a set of risk assessment criteria to determine if the information contained therein is subject to this GLBA Security Policy. Some of the most important criteria are: What abuses could the item be used for and how? (identity theft, credit fraud, stalking, spamming) How could the information be obtained? Is the information part of public records such as Register of Deeds recorded documents? What is the likelihood of theft or misuse? What security measures should we take? What impact does each have on business processes?

III. ROLES & RESPONSIBILITY

Securing the non-public information of our customers through regulating & monitoring security practices of all printed materials and the data contained in KBTG’s information systems is of the utmost importance. To effectively manage the security of non-public information, the assistance of all KBTG employees is required.

For proper handling and disposal of non-public information contained, amongst others, printed material and computer data accessed by some or all of KBTG’s employees; the following employees’ roles are defined as:

The Information Systems Manager (“IS Mgr”) is responsible for implementing and monitoring a consistent information security program as well as providing the necessary tools, equipment, and underlying infrastructure to comply with all aspects of KBTG’s security and privacy policies.

Branch and Department Managers (“Information Custodians”) are responsible for direct supervision of security practices in their respective department(s) or office(s).

Information Custodians:

Will follow the guidelines and monitor compliance of this policy for their office areas.

Will authorize information access for appropriate employees or third parties.

Will ensure that their subordinate personnel are aware of and understands all current and updated security policies.

Will notify the IS Mgr and recommend appropriate use(s) and protections of non-public information contained in new or updated forms, communications, data files, or business practices.

KBTG employees (“Users”) are responsible for securing all data they work with per the guidelines set forth by the IS Mgr. Users are also responsible to monitor fellow Users in their respective department(s) and office(s).

Users:

Will intervene and secure non-public information improperly secured by fellow Users.

Will instruct the offending User to ensure non-public information is secured properly in the future.

Will inform an Information Custodian and/or the IS Mgr in the event that a fellow User continues to improperly secure non-public information after being notified and properly re-trained by the User.

IV. **GENERAL PHYSICAL SECURITY MEASURES**

Each non-public information item is evaluated separately and secured appropriately; however KBTG also realizes that change is frequent and for the good of all parties.

Due to changes in our own practices as well as those of our customers and providers we cannot always make a formal assessment of the information on the spot. In these cases, Information Custodians and Users are empowered to notify the IS Mgr and make their own determination of whether the information should be secured on a temporary basis until a formal assessment can be done.

In general these new information types are similar in nature or content to previously assessed information materials and should be secured in a similar manner. KBTG takes a proactive stance to security believing that items not specifically covered by current laws, bills, acts, etc should still be evaluated for risk. We generally take ‘good sense’ security measures on these items until an industry standard is set forth concerning security of these information assets.

V. **GENERAL TECHNICAL SECURITY MEASURES**

Computer and Network Security is a vast ever-changing landscape in today’s tech savvy world; beyond the specific risks of certain provided documents and electronic files are more generalized risks including computer viruses, hackers, trojan horses, thieves, con-artists, etc.

KBTG recognizes these and other threats as well as the fact that often these threats are used together in a blended threat. To protect against blended threats, KBTG uses a multilayered approach to security that include physical locks, alarm systems, firewalls, password and use policies, employee training programs, regular backups, shredding of documents, expiration schedules and more.

VI. **AUDITING**

Every system and security measure can only be effective when properly monitored.

Electronic systems are regularly monitored in real time. Periodic audits of electronic systems may be done by KBTG Information Systems staff. KBTG may on occasion have external audits conducted by a reputable security firm considered 'specialists' in electronic systems security. Logs and/or reports from scheduled audits will be kept securely for a period of time determined by the ISMgr.

Official Audits for physical security measures and practices will be conducted at random unannounced intervals by the IS Mgr with the help of Information Custodians and other Users. A detailed log/report of each official audit will be kept on file for a period of time determined by the ISMgr.

In the event that an Information Custodian or User fails any part of an audit, the IS Mgr will provide what is necessary to meet all compliance requirements. A follow-up audit will be scheduled at random to ensure compliance.

VII. **SUMMARY**

KBTG is committed to protecting its customer's non-public information.

Any known violations of these policies should be reported to KBTG's IS Mgr (ISMgr@knightbarry.com). Violations of these policies can result in immediate disciplinary action in accordance with KBTG procedures. KBTG may advise law enforcement agencies when a criminal offense may have been committed or seek legal counsel for damages or perceived damages.

*For those institutions requiring additional GLBA compliance information please visit our website @ www.knightbarry.com to view our Privacy Policy and GLBA technical outline. More detailed documentation for certain aspects of our privacy and security program(s) may be made available under the supervision of the IS Mgr upon written request.

Questions regarding KBTG's GLBA Security Policy or Information Security Policies should be addressed to KBTG's IS Mgr. (ISMgr@knightbarry.com)