

# **Knight-Barry Title Group GLBA Technical Outline**

## **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.

This document provides an outline of the technology based security elements used by Knight-Barry to ensure GLBA requirements are met. This technical outline is a supplement to our GLBA Security Policy as supporting documentation for those who require it.

Our GLBA Security Policy can be found online at [www.knightbarry.com](http://www.knightbarry.com)

Enterprise systems security is a vast ever-changing landscape in today’s tech savvy world. As such, the most significant security items are addressed here in general so as not to compromise our technical security measures.

KBTG has assembled the following categories contained in this policy:

- I. Training**
- II. Physical Security Measures**
- III. General Computer and Network Security Measures**
- IV. Summary**

### **I. TRAINING**

Training is key to our privacy / security program. As such every new employee is provided an employee handbook that includes this and other information. Each employee will be provided written privacy and security supplements periodically in the form of interoffice mail, email, or posting on the KBTG intranet as such supplements are updated or added. Employees will be required to attend meetings or training sessions every year to cover these and other topics.

### **II. PHYSICAL SECURITY MEASURES**

During normal business hours each facility’s main entrance is controlled by a receptionist; additional entrances/exits are to remain locked as allowed by local fire code.

After hours, doors are locked and monitored by a security system; often motion detectors are used for additional protection. In certain areas, security systems are controlled by specialized zones and require limited individual passwords for disarming. A secured list is kept by the IS Mgr. or Information Custodian, who retain keys and security system clearance to every secured area or system.

In our industry, we are required to keep paper or electronic based records and originals of certain documents for varying lengths of time. KBTG has developed a classifications chart to determine what records must be kept, for how long, and how they must be secured.

Based on the chart, certain documents or electronic media must be kept in locked cabinets, secured file rooms, or safes. The bulk of long-term records storage should be kept at KBTG's headquarters location.

Certain documents must be destroyed on a timely basis. Some documents are paper and are shredded. Other documents are electronic and must be deleted from the computer system in which they reside.

In order to process customer requests for services, information must be unlocked and handled by the appropriate Users. We refer to this as Work in Process. KBTG has set forth guidelines on how many files containing non-public information may be out of secure locations yet still in Users secure possession. Other guidelines have been set forth regarding keeping a clean orderly work area as well as securing work areas and files. IT infrastructure assists the Users with measures including system inactivity timeouts, that require re-entry of password to resume access, and other measures where deemed necessary.

### **III. GENERAL COMPUTER AND NETWORK SECURITY MEASURES:**

KBTG recognizes that most threats to computer and network security are in the form of a Blended Threat. To protect against blended threats KBTG uses a multilayered approach to security. Some of those measures are:

Logon Warnings are used to deter unauthorized access and to remind Users of their responsibility to follow all company policies including privacy and security.

Two stage Antivirus (Virus / SPAM filtering at externally managed email server. Server and desktop Anti-virus programs.)

Wireless network access is permitted in some locations. In those locations wireless networks are secured with commercially acceptable encryption.

Computer systems are secured with unique UserID's and Passwords. Most systems lockout the UserID after 3 incorrect login attempts. All Users have signed a computer use policy agreement.

Firewalls secure our systems where appropriate. Communications are blocked unless specifically allowed by pre-set firewall rules.

Servers and Firewalls are patched regularly with Security Patches to defend against vulnerabilities as they are discovered. Depending which programs are affected, Users may be provided instructions for proper updating when a centrally controlled update process is not available.

The Knightbarry.com website and the information contained therein are considered public and, as such, have minimal controls to public information. KBTG's online production systems are secured by passwords and firewall controls even though information contained within those systems is part of or will become part of public record. Customers who are provided UserIDs/passwords are asked not to share them with others or write them down.

KBTG keeps data Backups, according to schedules, of critical data in the event of loss or damage. PC Users are instructed to backup data as necessary from their personal hard drives. Backup media containing non-public information is secured in server rooms or safes.

#### IV. **Summary:**

Protection of non-public information is a top priority for KBTG.

Any known violations of these policies should be reported to KBTG's IS Mgr ( [ISMgr@knightbarry.com](mailto: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](http://www.knightbarry.com) to view our Privacy Policy and GLBA Security Policy. 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](mailto:ISMgr@knightbarry.com) )