Non-Public Information Security and Disposal Policy

Purpose

This document establishes the corporate policy and standards for securing and disposing non-public information (NPI) at Crawford Law Group.

NPI includes any paper or electronic records produced by or in the possession of Crawford Law Group including, but not limited to, title, escrow, mortgage, insurance, and claims documents that contain

- Competitive data including, but not limited to, proprietary financial information, source code for software applications, data on acquisitions or mergers, and customer lists
- Legally sensitive data including, but not limited to, personnel information, legal investigations, and pending lawsuits
- Personal technology data including, but not limited to, specific system architecture information, IP addresses, user names/IDs, personal identification numbers (PINs), market IDs, certificates, security codes, access codes, password information, and answers to password hint questions (for example, mother's maiden name)
- Lender-supplied Disclosure Data including data transmitted on Good Faith Estimates, Truth-in-Lending Disclosures, and Closing Disclosure forms, when mandated by the Consumer Financial Protection Bureau, whether supplied in an electronic document or data format
- Loan-related documents including the FNMA 1003, Note, Deed of Trust, etc. known as "Loan Docs" transmitted by the lender to the settlement agent in preparation for borrower signing
- Non-public and personally identifiable information about an individual including, but not limited to, date of birth, Social Security numbers, passport identification numbers, driver's license numbers, state identification card numbers, credit or debit card numbers and expiration dates, bank account numbers, bank routing information, credit information, loan numbers and applications, account histories, and related personal and financial information
- Any other non-public, proprietary or secret information, or information identified as confidential

Policy

All Crawford Law Group employees are responsible for following the standards defined in this document.

Physical Security

Physical security for NPI must adhere to these standards:

- Restrict access to NPI to authorized employees only.
- Institute a "clean desk" policy requiring employees to close files containing NPI when they are away from their desks.
- Secure onsite documents, portable devices, and electronic media containing NPI in a desk, file cabinet, or locked room outside of normal business hours.

- Secure offsite documents in a commercial storage facility that is
  - Climate controlled
  - Equipped with a monitored security alarm
- Prohibit or control the use of removable media such as USB drives and external backup drives, unless encrypted.
- Prohibit NPI from being accessed with or stored on non-approved electronic devices.
- Use only secure delivery methods when mailing NPI. Secure delivery methods include
  - Inter-office mail—Sealed envelopes
  - External mail—Registered mail services (FedEx, UPS) with sealed envelopes and signature requirement
    Note: Large quantities of protected documents may only be shipped using a professional document management company that has been approved by management.
- Send faxes only to private or secure fax machines.
- Pick up and dispose of printer, fax, and copier output in a timely manner.
- Never leave documents, portable devices, or electronic media containing NPI in an unlocked vehicle or where they are visible from outside a locked vehicle.
- Never leave any item containing NPI unattended in a hotel room, conference room, reception area, or any other location that can be accessed by others.

Electronic Security

Electronic access or storage of NPI must adhere to these standards:

- Computer policies
  - Use strong passwords (8+ characters including numbers, symbols, and upper and lowercase letters) and require frequent password updates.
  - Require password-activated screen savers when employees leave their workstation.
  - Establish dedicated workstations for electronic banking.
  - Install and maintain up-to-date firewall, anti-virus, and other intrusion prevention systems.
  - Use data encryption for transmitting files containing NPI.
- Electronic communication such as e-mail, instant messaging, and texting.
  - Transmit NPI and money via Transport Layer Security Protocal (TLS) connections, password-protected attachments such as ShareFile, or other secure methods. Crawford Law Group utilizes Mircrosoft Office 365 to assist in the care of NPI.
  - Omit or obscure NPI.
  - Beware of “Phishing” e-mail messages which can appear to be from a trustworthy source, but are designed to trick the recipient into providing sensitive, private and confidential information. After clicking on an active link in a phishing e-mail, the recipient may be directed to a fraudulent website that attempts to acquire personal or private information or possibly infect the recipient’s computer with a hidden, sometimes undetectable, virus or malware.

Note: To check the destination of an active link, you should hover your mouse over the link and review the address information displayed in the status bar located at the bottom of the browser page.

- Portable storage
  - Encrypt or password-protect documents containing NPI on portable devices such as laptops, smart phones, USB drives, and external backup drives.
  - Store portable devices securely to prevent theft or unauthorized access.
  - Secure portable devices as one would a computer.
- Websites
  - Enable encryption for company websites that collect NPI. When using trusted third-party websites, users should check for the padlock icon at the bottom right of the browser window or look for “https” instead of “http” in the address bar.
  - Avoid entering NPI in third-party websites that you do not trust. Especially when following links, users should always check the address bar to ensure that they have not been directed to a look-alike website.
  - Do not use public file storage or transfer services such as LeapFILE, FindMyFile, SendSpace, or DropBox for any files containing NPI.
  - Download, install, and update computer software only when instructed. Please consult the IT manager orpaul Flamand our IT specialist.
- File servers
  - Physically secure all servers in a locked room with limited and controlled access.
  - Limit access to directories, file shares, databases, and critical applications containing NPI to only those persons who require access for legitimate business purposes.
  - Ensure that server backups are encrypted.

Disposal

Federal law requires companies that possess NPI for a business purpose to dispose of the NPI, after business and regulatory retention requirements have been met, in a manner that protects against unauthorized access to or use of the information in connection with its disposal.

Some examples of appropriate disposal policies include

- Establish a document retention period that sets timelines for the disposal of NPI based on state requirements.
- Burn, pulverize, or shred hard copy records using a commercial shredder or a shredding company that has been approved by management.
- Destroy, degauss, or securely overwrite with a multiple-pass process all electronic files on decommissioned equipment including, but not limited to, computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, and cell phones.

Violation of Policy

Failure to adhere to all requirements stipulated in this policy and all related documents may result in disciplinary actions, up to and including

- Immediate removal of any applicable hardware/software/access to the Company Name computer network or business systems
- Formally reporting the incident to Crawford Law Group senior management
- Termination of employment
- Any other action deemed necessary by Crawford Law Group senior management

Review

Crawford Law Group has voluntarily adopted this policy for its sole and exclusive use. This policy and all related documents will be reviewed annually or as needed based on prevailing business conditions.

Approved

James B. Crawford, III, Managing Member

Revision History

Version Number	Revised Date	Effective Date	Approved By	Brief Change Summary
001	12-29-2014	12-29-2014	JBCIII	Original