Information Security Policy Handbook For Circle Mortgage Group

Circle Mortgage Group
500 Mamarock Avenue Suite 320 Harrison, NY 10528

Introduction

The Circle Mortgage Group Information Security and Confidentiality Policies are intended to define the handling and safeguarding of confidential financial and personal information and the relative sensitivity of information that should not be disclosed outside of the company without proper authorization. Please read this entire document and all of the information security polices contained in this document.

This document also defines the actions to be taken in the event data is improperly handled or a breach in data security occurs. The data includes that from all sources including company, clients, third-party vendors and partnerships.

The information covered in these policies includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect our company and client confidential information.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to the company Security Manager.

All company information is categorized into two main classifications:

1. Company Public
2. Company Confidential
    a. Company Corporate Data
    b. Contractual Data for Clients, Partnerships and Third-Party Vendors
    c. Client Data under the Control of company

Company Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Company.

Company Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in Company Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Company Confidential information is "Company Third Party Confidential" information. This is confidential information belonging or pertaining to another Corporation or client which has been entrusted to Company by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from corporate data, client/mortgage borrower data, and joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Company network to support our operations.

Company follows the requirements for financial organizations as defined by The Gramm-Leach-Bliley Act (GLB Act), 15 U.S.C. 6801, implemented by 16 CFR Part 314 and The Federal Trade Commission (FTC) Rule on "Standards for Safeguarding Customer Information" Company personnel are encouraged to use common sense judgment in securing company information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

1. Table of Contents

2. Acceptable Use Policy

Circle Mortgage Group with ABT is hereinafter referred to as "the company."

2.1 Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

2.2 Purpose

Since inappropriate use of corporate systems exposes the company to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

2.3 Scope

The scope of this policy includes any and all use of corporate IT resources, including but not limited to, computer systems, email, the network, and the corporate Internet connection. Use of the PowerCore® Mortgage Cloud, MortgageWorkspace™, DeviceGuardian™, and EmailGuardian™ in combination with following these security policies brings a user's practices into compliance with the regulatory security requirements and best practices of the mortgage industry.

2.4 Policy

2.4.1 E-mail Use

Personal usage of company email systems is permitted as long as A) such usage does not negatively impact the corporate computer network, and B) such usage does not negatively impact the user's job performance.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the company may not be sent via email, regardless of the recipient, without proper encryption. When confidential information needs to be sent via email that email will be sent using EmailGuardian™ for secure and encrypted emails.
- It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. When large files need to be sent via email that email will be sent using EmailGuardian™ for large attachments.

Please note that detailed information about the use of email may be covered in the company's Email Policy.

2.4.2 Confidentiality

Confidential data must not be A) shared or disclosed in any manner to non-employees of the company, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

2.4.3 Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access. Users should access the network using MortgageWorkspace™ with DeviceGuardian™ installed and work exclusively in this environment.

2.4.4 Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
- Install or distribute unlicensed or "pirated" software.
- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.
- Access the network outside of either the PowerCore Secure Desktop or move any data out of this secure environment.

2.4.5 Blogging and Social Networking

Blogging and social networking by the company's employees are subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging and social networking is never allowed from the corporate computer network. In no blog or website, including blogs or sites published from personal or public systems, shall the company be identified, company business matters discussed, or material detrimental to the company published. The user must not identify himself or herself as an employee of the company in a blog or on a social networking site. The user assumes all risks associated with blogging and/or social networking.

2.4.6 Instant Messaging

Instant Messaging is allowed for corporate communications only using the instant messaging software provided by MortgageWorkspace™. The user should recognize that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

2.4.7 Overuse

Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted.

2.4.8 Web Browsing

The Internet is a network of interconnected computers of which the company has very little control. The employee should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. The company is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

Web browsing should be performed in MortgageWorkspace™ where Internet traffic and browsing is controlled and secured, restricting access to sites appropriate for the workplace.

Personal Use. The company recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of company computer systems to access the Internet is permitted during lunch, breaks, and before/after business hours, as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the company or on the user's job performance.

2.4.9 Copyright Infringement

The company's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

2.4.10 Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the corporate network under any circumstance.

2.4.11 Streaming Media

Streaming media is not permitted for any purpose.

2.4.12 Monitoring and Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor any and all use of the computer network. To ensure compliance with

company policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

2.4.13 Bandwidth Usage

Excessive use of company bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low company-wide usage.

2.4.14 Personal Usage

Personal usage of company computer systems is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the company or on the user's job performance.

2.4.15 Remote Desktop Access

Use of remote desktop software and/or services is allowable as long as it is provided by the company such as MortgageWorkspace™. Remote access to the network must conform to the company's Remote Access Policy.

2.4.16 Circumvention of Security

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

2.4.17 Use for Illegal Activities

No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes
- Downloading, storing, or distributing copyrighted material

The company will take all necessary steps to report and prosecute any violations of this policy.

2.4.18 Non-Company-Owned Equipment

The user must obtain written permission from company before installing outside or non-company-provided computer systems on the company network. Once this permission is obtained, and dependent on any conditions granted along with such permission, the user can connect a non-company-owned system to the network. Precautions must be taken, by the installation of DeviceGuardian™ onto the non-company-owned equipment to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the company network.

2.4.19 Personal Storage Media

Personal storage devices represent a serious threat to data security and are expressly prohibited on the company's network.

2.4.20 Software Installation

Installation of non-company-supplied programs is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.

2.4.21 Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains company information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user's password over the telephone or by email.
- Any other suspicious event that may impact the company's information security.

Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

2.4.22 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

2.5 Enforcement

This policy will be enforced by company. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

2.6 Definitions

Blogging – The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

DeviceGuardian™ – is a cloud based local software tool designed for the mortgage industry that manages and provides the security of your local device including your laptop, desktop, tablet and phone. You are required to have this software installed on any device that accesses the company network, software or data.

Instant Messaging – A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

EmailGuardian™ – ABT's hosted email system that complies with regulatory demands for email security and provides complete protection from spam, viruses, malware, phishing, data leaks and email transmission encryption policies.

Peer-to-Peer (P2P) File Sharing – A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

MortgageWorkspace™ – is provided as a cloud service or a tool installed on your device that securely manages all of your mortgage software, data, and security configurations in a secured desktop environment. MortgageWorkspace™ along with these security policies helps you comply with mortgage specific information security regulations and best practices.

Remote Desktop Access – Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Streaming Media – Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

3. Confidential Data Policy

Circle Mortgage Group with ABT is hereinafter referred to as "the company."

3.1 Overview

Confidential data is typically the data that holds the most value to a company. Often, confidential data is valuable to others as well, and thus can carry greater risk than general company data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

3.2 Purpose

The purpose of this policy is to detail how confidential data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of confidential data, and outlines specific security controls to protect this data.

3.3 Scope

The scope of this policy covers all company-confidential data, regardless of location. All electronic forms of data must be kept within MortgageWorkspace™ and EmailGuardian™. Also covered by the policy are hardcopies of company data, such as printouts, faxes, notes, etc.

3.4 Policy

3.4.1 Treatment of Confidential Data

For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Policy.

3.4.1.1 Storage

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

3.4.1.2 Transmission

Confidential data must not be 1) transmitted outside the company network without the use of strong encryption, 2) left on voicemail systems, either inside or outside the company's network.

3.4.1.3 Destruction

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.
- Storage media (CD's, DVD's): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the company must use the most secure commercially-available methods for data wiping. Alternatively, the company has the option of physically destroying the storage media.

3.4.2 Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to the company's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential."
- Users must only access confidential data to perform his/her job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.
- If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Refer to the company's outsourcing policy for additional guidance.

3.4.3 Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity. The company requires that the following guidelines are followed:

- Strong Encryption. Strong encryption must be used for confidential data transmitted external to the company. If confidential data is stored on laptops or other mobile devices, it must be stored in encrypted form.
- Network Segmentation. Separating confidential data by network segmentation is strongly encouraged.
- Authentication. Strong passwords must be used for access to confidential data.
- Physical Security. Systems that contain confidential data should be reasonably secured.
- Printing. When printing confidential data, the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas.
- Faxing. When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.

- Emailing. Confidential data must not be emailed outside the company without the use of strong encryption.
- Mailing. If confidential information is sent outside the company, the user must use a service that requires a signature for receipt of that information.
- Discussion. When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.
- Confidential data must be removed from documents unless its inclusion is absolutely necessary.
- Confidential data must never be stored on non-company-provided machines (i.e., home computers).
- If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

3.4.4 Examples of Confidential Data

The following list is not intended to be exhaustive, but should provide the company with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee or customer social security numbers or personal information
- All mortgage loan and related customer documentation
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)
- Customer data
- Company financial data (if company is closely held)
- Sales forecasts
- Product and/or service plans, details, and schematics,
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

3.4.5 Emergency Access to Data

A procedure for accessing confidential and critical data during an emergency is often a good idea if the company handles information that is integral to the health, well-being, or protection of other persons or entities. If the company maintains this type of data, it should consider establishing such a procedure in case the normal mechanism for access to the data becomes unavailable or disabled due to system or network problems.

3.4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

3.5 Enforcement

This policy will be enforced by the ABT Technical Support and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

3.6 Definitions

Authentication – A security method used to verify the identity of a user and authorize access to a system or network.

Encryption – The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Data Device – A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

MortgageWorkspace™ – is provided as a cloud service or a tool installed on your device that securely manages all of your mortgage software, data, and security configurations in a secured desktop environment. MortgageWorkspace™ along with these security policies helps you comply with mortgage specific information security regulations and best practices.

Two-Factor Authentication – A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

4. Password Policy

Circle Mortgage Group with ABT is hereinafter referred to as "the company."

4.1 Overview

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

4.2 Purpose

The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

4.3 Scope

This policy applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

4.4 Policy

4.4.1 Construction

The best security against a password incident is simple: following a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction:

- Passwords should be at least 8 characters
- Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
- Passwords should be comprised of a mix of upper and lower case characters
- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this way as well, for example an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

4.4.2 Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

- Users must not disclose their passwords to anyone
- Users must not share their passwords with others (co-workers, supervisors, family, etc.)
- Users must not write down their passwords and leave them unsecured
- Users must not check the "save password" box when authenticating to applications
- Users must not use the same password for different systems and/or accounts

- Users must not send passwords via email
- Users must not re-use passwords

4.4.3 Change Frequency

In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a mini

mum, users must change passwords every 90 days. The company uses MortgageWorkspace™ to help enforce this policy by expiring users' passwords after this time period. However, the user still needs to change passwords in other company systems manually.

4.4.4 Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the Executive Team and/or ABT technical support. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised the ABT technical support team will request that the user, or users, change all his or her passwords.

4.4.5 Applicability of Other Policies

This document is part of the organization's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

4.5 Enforcement

This policy will be enforced by the ABT technical support and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company

property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

4.6 Definitions

Authentication – A security method used to verify the identity of a user and authorize access to a system or network.

Password – A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

MortgageWorkspace™ – is provided as a cloud service or a tool installed on your device that securely manages all of your mortgage software, data, and security configurations in a secured desktop environment. MortgageWorkspace™ along with these security policies helps you comply with mortgage specific information security regulations and best practices.

Two Factor Authentication – A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

5. Mobile Device Policy

Circle Mortgage Group with ABT is hereinafter referred to as "the company."

5.1 Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

5.2 Purpose

The purpose of this policy is to specify company standards for the use and security of mobile devices.

5.3 Scope

This policy applies to company data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with company data.

5.4 Policy

5.4.1 Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The company should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

- Laptop locks and cables can be used to secure laptops when in the office or other fixed locations.
- Mobile devices should be kept out of sight when not in use.
- Care should be given when using or transporting mobile devices in busy areas.
- As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.
- The company should evaluate the data that will be stored on mobile devices and consider remote wipe/remote delete technology. This technology allows a user or administrator to make the data on the mobile device unrecoverable.
- The company should continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

5.4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting company data. The following sections specify the company's requirements for data security as it relates to mobile devices.

5.4.2.1 Laptops

Whole disk encryption is required. Laptops must require a username and password or biometrics for login. DeviceGuardian™ must be installed on all devices.

5.4.2.2 PDAs/Smart Phones

Encryption and login passwords are required on PDAs/smart phones. DeviceGuardian™ must be installed on all devices.

5.4.2.3 Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storing company data on such devices is not permitted under any circumstance.

5.4.2.4 Portable Media Players

No company data can be stored on personal media players.

5.4.2.5 Other Mobile Devices

Unless specifically addressed by this policy, storing company data on other mobile devices, or connecting such devices to company systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the ABT Technical Support and/or the Executive Team.

5.4.3 Connecting to Unsecured Networks

Users must not connect to any outside network without a DeviceGuardian™ installed on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the company.

5.4.4 General Guidelines

The following guidelines apply to the use of mobile devices:

- Loss, Theft, or other security incident related to a company-provided mobile device must be reported promptly.

- Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device, it must be appropriately secured with DeviceGuardian™ and comply with the Confidential Data policy.
- Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.
- Users are not to store company data on non-company-provided mobile equipment. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA.

5.4.5 Audits

The company must conduct periodic reviews to ensure policy compliance. A sampling of mobile devices must be taken and audited against this policy on a quarterly basis.

5.4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.5 Enforcement

This policy will be enforced by the ABT Technical Support and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

5.6 Definitions

Encryption – The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

DeviceGuardian™ – is a cloud based local software tool designed for the mortgage industry that manages and provides the security of your local device including your laptop, desktop, tablet and phone. You are required to have this software installed on any device that accesses the company network, software or data.

Mobile Devices – A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Mobile Storage Media – A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Password – A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

PDA – Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Portable Media Player – A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

MortgageWorkspace™ is provided as a cloud service or a tool installed on your device that securely manages all of your mortgage software, data, and security configurations in a secured desktop environment. MortgageWorkspace™ along with these security policies helps you comply with mortgage specific information security regulations and best practices.

Smartphone – A mobile telephone that offers additional applications, such as PDA functions and email.

6. Remote Access Policy

Circle Mortgage Group with ABT is hereinafter referred to as "the company."

6.1 Overview

It is often necessary to provide access to corporate information resources to employees or others working outside the company's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

6.2 Purpose

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

6.3 Scope

The scope of this policy covers all employees, contractors, and external parties that access company resources over a third-party network, whether such access is performed with company-provided or non-company-provided equipment.

6.4 Policy

6.4.1 Prohibited Actions

Remote access to corporate systems is only to allowed through MortgageWorkspace™ from a device with DeviceGuardian™ installed.

The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a company system without the approval of ABT Technical Support or the Executive Team.
- Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the Executive Team.
- Use of non-company-provided remote access software.
- Split Tunneling to connect to an insecure network in addition to the corporate network, or in order to bypass security restrictions.

6.4.2 Use of non-company-provided Machines

Accessing the corporate network through home or public machines can present a security risk, as the company cannot completely control the security of the system accessing the network. Use of non-company-provided machines to access the corporate network is permitted as long as PowerCore Secure Desktop is installed, and as long as the machine meets the following criteria:

- It has up-to-date antivirus software installed
- Its software patch levels are current
- It is protected by a firewall

When accessing the network remotely, users must not store confidential information on home or public machines.

6.4.3 Client Software

The company will supply users with MortgageWorkspace™ and DeviceGuardian™ that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access.

6.4.4 Network Access

The company will limit remote users' access privileges to only those information assets that are reasonable and necessary to perform his or her job function when working remotely (i.e., email). The entire network must not be exposed to remote access connections.

6.4.5 Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the company's network must be timed out after 2 hours of inactivity.

6.4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

6.5 Enforcement

This policy will be enforced by the ABT Technical Support and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.6 Definitions

DeviceGuardian™ – is a cloud based local software tool designed for the mortgage industry that manages and provides the security of your local device including your laptop, desktop, tablet and phone. You are required to have this software installed on any device that accesses the company network, software or data.

Modem – A hardware device that allows a computer to send and receive digital information over a telephone line.

Remote Access – The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

MortgageWorkspace™ – is provided as a cloud service or a tool installed on your device that securely manages all of your mortgage software, data, and security configurations in a secured desktop environment. MortgageWorkspace™ along with these security policies helps you comply with mortgage specific information security regulations and best practices.

Split Tunneling – A method of accessing a local network and a public network, such as the Internet, using the same connection.

Timeout – A technique that drops or closes a connection after a certain period of inactivity.

Two Factor Authentication – A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7. Backup Policy

Circle Mortgage Group with ABT is hereinafter referred to as "the company."

7.1 Overview

A backup policy is similar to an insurance policy - it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document. A company's backup policy is among its most important policies.

7.2 Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

7.3 Scope

This policy applies to all data stored within MortgageWorkspace™ and EmailGuardian™. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

7.4 Policy

7.4.1 Identification of Critical Data

The company must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

7.4.2 Data to be Backed Up

A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

- All data determined to be critical to company operation and/or employee job function.
- All information stored on the corporate file server(s) and email server(s). It is the user's responsibility to ensure all data is kept only in the MortgageWorkspace™, and within the EmailGuardian™.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

7.4.3 Backup Frequency

Backup frequency is critical to successful data recovery. The company has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

File data	Full: every day	
SQL data	Incremental: every 4 hours	Full: every day
Email data	Incremental: every 4 hours	Full: every day

7.4.4 Off-Site Rotation

Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the company's uptime requirements. The company has determined that backup media must be rotated off-site at least once per month. A month-end snapshot for backed up data is written onto tape and taken off site for secure storage.

7.4.5 Backup Storage

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, company data, precautions must be taken that are commensurate to the type of data being stored. The company has set the following guidelines for backup storage.

When stored onsite, backup media must be stored in a fireproof container in an access-controlled area. When shipped offsite, a hardened facility (i.e., commercial backup service) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media. If a backup service is used, rigorous security procedures must be developed and maintained, which will include, at minimum, credential-verification and signature of the backup service courier. Online backups are allowable if the service meets the criteria specified herein. Confidential data must be encrypted using industry-standard algorithms to protect the company against data loss.

7.4.6 Backup Retention

When determining the time required for backup retention, the company must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The company has determined that the following will meet all requirements (note that the backup retention policy must confirm to the company's data retention policy and any industry regulations, if applicable):

Incremental Backups must be saved for one month.

Full Backups must be saved for six months.

Monthly Backups must be saved for seven years.

7.4.7 Restoration Procedures & Documentation

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.

7.4.8 Restoration Testing

Since a backup policy does no good if the restoration process fails it is important to periodically test the restore procedures to eliminate potential problems.

Backup restores must be tested when any change is made that may affect the backup system, as well as once every month.

7.4.9 Expiration of Backup Media

Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

7.4.10 Applicability of Other Policies

This document is part of ABT's MortgageWorkspace™ and EmailGuardian™'cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

7.5 Enforcement

This policy will be enforced by ABT and the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

7.6 Definitions

Backup – To copy data to a second location, solely for the purpose of safe keeping of that data.

Backup Media – Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.

Full Back Up – A backup that makes a complete copy of the target data.

Incremental Backup – A backup that only backs up files that have changed in a designated time period, typically since the last backup was run.

EmailGuardian™ – ABT's hosted email system that complies with regulatory demands for email security and provides complete protection from spam, viruses, malware, phishing, data leaks and email transmission encryption policies.

MortgageWorkspace™ – is provided as a cloud service or a tool installed on your device that securely manages all of your mortgage software, data, and security configurations in a secured desktop environment. MortgageWorkspace™ along with these security policies helps you comply with mortgage specific information security regulations and best practices.

Restoration – Also called "recovery." The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

8. Retention Policy

Circle Mortgage Group with ABT is hereinafter referred to as "the company."

8.1 Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the company's guidelines on retention are consistently applied throughout the organization.

8.2 Purpose

The purpose of this policy is to specify the company's guidelines for retaining different types of data.

8.3 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.

Note that the need to retain certain information can be mandated by local, industry, or federal regulations. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

8.4 Policy

8.4.1 Reasons for Data Retention

The company does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective, and would place an excessive burden on the IT Staff to manage the constantly-growing amount of data.

Some data, however, must be retained in order to protect the company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation

8.4.2 Data Duplication

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying the company's data, it is important to also understand where that data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of the information.

8.4.3 Retention Requirements

This section sets guidelines for retaining the different types of company data.

Personal – There are no retention requirements for personal data. In fact, the company requires that it be deleted or destroyed when it is no longer needed.

Public – Public data must be retained for 3 years.

Operational – Most company data will fall in this category. Operational data must be retained for 5 years.

Critical – Critical data must be retained for 7 years.

Confidential – Confidential data must be retained for 7 years.

8.4.4 Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

8.4.5 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the company will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, the company must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the company's executive team.

The company specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or company policy.

8.4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

8.5 Enforcement

This policy will be enforced by ABT Technical Support Manager and/or the Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

8.6 Definitions

Backup – To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption – The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Encryption Key – An alphanumeric series of characters that enables data to be encrypted and decrypted.

Policy Acknowledgement Form

Company:	**Circle Mortgage Group**
User Name:	
Department:	

I understand that being granted access to computer systems and company information carries a great deal of responsibility. I recognize that I am being granted this access with the understanding that I will

use the network resources and company information in a responsible manner. I realize that specific guidelines and expectations of me are detailed in the appropriate policies.

I UNDERSTAND THAT WHILE THE COMPANY INTENDS TO PROVIDE A SAFE AND POSITIVE EXPERIENCE WHEN USING COMPANY SYSTEMS AND THE INTERNET, THE COMPANY MAKES NO WARRANTIES AS TO THE CONTENT OF THE NETWORK AND THE INTERNET.

I AM RESPONSBILE FOR MY OWN ACTIONS AND WILL RELEASE THE COMPANY FROM ANY LIABILITY RELATING TO MY NETWORK USAGE. I AGREE TO USE THE NETWORK AND SYSTEMS IN AN APPROPRIATE MANNER AS SPECIFIED IN THE APPLICABLE POLICIES. I UNDERSTAND THAT MY USE OF THE NETWORK AND SYSTEMS MAY BE MONITORED AT ANY TIME AND I SHOULD HAVE NO EXPECTATION OF PRIVACY IN CONNECTION WITH THIS USE.

I UNDERSTAND THAT FAILURE TO USE THE NETWORK IN A RESPONSBILE MANNER MAY RESULT IN LOSS OF NETWORK PRIVELEGES, SUSPENSION, OR TERMINATION. I UNDERSTAND THAT IF ILLEGAL ACTIVITY IS SUSPECTED, THE COMPANY WILL REPORT THE ACTIVITY TO THE APPLICABLE AUTHORITIES.

User Name (Print): _____

User Signature: _____

Date: _____