ABBM

44 Cook St Ste 100
Denver, CO 80206

abiggerbettermortgage.com o-970-476-5547 f-303-496-1800 abiggerbettermortgage@gmail.com NMLS# 2522067

A BIGGER BETTER MORTGAGE

DATA SECURITY AND RETENTION POLICY AND PROCEDURES

2025

Table of Contents

INTRODUCTION

This policy is NOT shared with the public. If in the wrong hands, it could be a threat to our company data and a threat to its consumer and business customers. In short, we are not handing a cyber criminal information that will help them break in and steal confidential and personal information that was entrusted to A Bigger Better Mortgage as it is our job to protect that information and earn the trust of our customers.

This policy lays out how we protect, retain and destroy consumer data. It is very confidential and is not to be distributed to anyone other than those who it has been given to directly from an officer of A Bigger Better Mortgage or its DBAs.

If it is found that any business this is shared with has distributed a copy of this policy, it could mean termination of the relationship. If any employee distributes this policy without or written consent it will mean termination for that employee.

Gramm-Leach-Bliley Act is federal legislation that mandates financial institutions to be transparent about their information-sharing practices and to take robust measures to secure sensitive consumer data. In the context of GLBA, financial institutions are defined as organizations offering consumer-focused financial products or services, such as loans, investments, financial advice, and insurance.

Gramm-Leach-Bliley Act (GLBA) underwent substantial updates that took effect on June 9, 2023. Considering these amendments, financial organizations must recalibrate their practices to maintain compliance to help successfully navigate regulatory audits.

The GLBA Safeguards Rule is a regulatory framework that requires financial institutions to protect customer data. It's part of the Gramm-Leach-Bliley Act (GLBA), which requires institutions to protect consumers' personal information and privacy.

- The Pretexting Provisions: These clauses explicitly prohibit the practice of pretexting, defined as the act of obtaining private information through deceptive or false pretenses.

What is the Safeguards Rule?

The GLBA Safeguards Rule is a regulatory framework that mandates financial institutions to implement comprehensive security measures for protecting customer data. Originally established in 2003 and known formally as the Standards for Safeguarding Customer Information, the rule outlines a multi-layered approach involving administrative, technical, and physical safeguards.

Its primary goal is to ensure the security and privacy of customer information. The Federal Trade Commission (FTC) most recently updated these guidelines on December 9, 2021, with the amendments, termed the Final Rule, becoming effective on June 9, 2023.

Confidential Data Collected but Not Limited to:

- Bank account and retirement statements
- Social Security information
- Identification, ID, driver's license, green card, passport, birth certificates
- Birthdates
- Addresses
- Credit reports
- Age, Gender and Ethnicity per HMDA
- IRS and state tax returns
- Income documents, W2’s, 1099’s, paystubs, child support, retirement.
- Legal Records: Title reports, tax certifications, title vesting, deeds, notes, death certificates, PR appointments, POA, DD4, COE and other legal documents.

Employee Information Retention

Because employees as Loan Originators must also keep records by law and have the same retention requirements as the business does. We require them to have certain securities, however, we do not expect them to have separated servers or computers to safeguard customer data or to follow the same protocol on their personal computers.

Employees must install:

- Have Bitdefender
- Ad blocker
- Decentraleyes
- Password protected
- KeePassXC (encrypted password ledger) not held by browser, for any passwords that need to be protected. They may also keep them in a notebook or folder in a locked box or filing cabinet if they work from home.
- We recommend Brave as a browser but do not require it
- All files must be sent to us after they are closed and no longer considered a working file

Working File Retention

A working folder is a file that is in progress and is not ready to be closed and archived. All working files are stored on a separate hard drive that can be removed at the end of the work day and stored in a secure environment. These working folders are password protected and encrypted and can be used in windows with password protected folder after it is setup in Linux, windows does not password protected or encrypt folders, it must be done in Linux OS.

The working file may be open during use but once closed, it will require the password again.

Archival Data

Historical Financial Records

After the file is close and we are no longer working the file, it is moved to an isolated offline Air-Gapped system (isolated computer) that is Linux based where the folder that holds that file is password protected, and thus encrypted. The passwords to those encrypted files are held in KeePassXC using a two way password to access the KeePassXC database with a YubiKey which is a flash drive which has it's own password that acts a secondary password to KeePassXC. We told KeePassXC that it will not grant access without the YubiKey flash drive which has it's own password thus making it impossible to access the password for the files. If you had the password to the KeePassXC database you would not be able to access it without the YubiKey flash drive, which is kept in a safe or lockbox. Even with the YubiKey, you would still need to know the primary password to access the database.

The lock and key are separated to retrieve the password to the file(s) from KeePassXC, which is not install on the same computer that holds the protected files. If someone tried to access the files on the Linux based computer they would only see password protected encrypted folders and nothing else, so they would not know that we are saving passwords for those files on KeePassXC.

Secure File Transfer

The files are transferred from the working computer to the Linux computer via flash drive which is where the working folders are stored. We use something like Parted Majic to destroy the data from the flash drive after the file is moved.

Who Has Access and Knowledge

President Bailey Campbell and Vice President Jessy Campbell

Retention Period

- **All completed and closed** loan files will be kept for seven years
- **Denied for a loan** will be kept for two to three years because the inquiry stays on the credit for two years.
- **Closing Disclosures** must be kept for a minimum of five years.
- **Loan Estimates** must be kept for a minimum of three years after the date the loan has closed.

Destruction of Files

In Linux there are six ways to destroy a file from the hard drive, we use *Shred*.

Shred Command in Linux with Examples

When you delete a file from Linux or from any Operating System, then the file is not deleted permanently from the hard disk. When a file is deleted, it first gets moved to the trash and as soon as you clear off the trash the files get deleted for the file system. But the file is still there on your hard drive, and it could be recovered. When you delete a file permanently or delete it from the trash, the pointer pointing to the file leaves the address of it and the data of the file is sent to a sector in hard disk and is considered as unallocated space and it can be recovered easily. The file gets permanently deleted when the OS writes over the sector of the file which was considered as unallocated. So, in order to delete a file completely from a hard disk "**shred**" is used in Linux. This command overwrites the contents of a file multiple times, using patterns chosen to maximize the destruction of the residual data, making it harder for even very expensive hardware probing to recover it.

Syntax of the `shred` command in Linux

```
shred [OPTION] FILE
```

[OPTIONS] represents the various parameters and flags that can be used to modify the behavior of the Shred command

FILE refers to the file or files you wish to shred.

Options available in `shred` Command

Options	**Description**
-n, –iterations=N	This option allows you to specify the number of times the file will be overwritten during the shredding process. By default, Shred performs 3 iterations.
-u, –remove	This option instructs Shred to remove the file after the shredding process is complete.
-v, –verbose	When using this option, Shred provides detailed information about the shredding process.

Options	**Description**
-z, –zero	This option adds a final overwrite of all zeros to the file after the shredding process is complete. This helps to hide the fact that the file has been shredded.
-f, –force	This option forces Shred to shred files that have read-only permissions or are otherwise protected.
-r, –random-source=FILE	With this option, you can specify a file as the source of random data for overwriting the file being shredded.

To permanently delete a file from a Linux hard drive, you can use the rm command, the unlink command, or a secure deletion tool.

Internet Browsing Attacks

The first and foremost vector of attack from malware that can compromise your system's information is the Internet. There is no doing business in the modern world without use of the Internet to some capacity or another, it's the highest profile target method of accessing private information & is therefore paramount to not only ensure secure browsing but to also include as many layers of security possible. The more layers of security you have, the less vulnerable your system is to a breach.

Choice of Browser

Browsers are what are used to browse the Internet. This includes your typical mainstays such as Internet Explorer and Google Chrome. However, not all browsers are made equal, and some are more secure & versatile than others. Some are known for conducting suspicious activity, such as Opera, which has a reputation of spying on its users and selling their data. Chrome is notorious for being a RAM hog.

Brave

Brave is the most secure and privacy intensive browser to date, coming prepackaged with ad block, script block & tracking block. Firefox, however, is currently the fastest & most versatile browser you can find, but does not come with the same security measures as Brave preinstalled. Whatever browser you choose to use, it is important to make sure you have personally implemented the correct security measures for that browser and in fact, all browsers present on your system.

Browser Hardening

Browser hardening is the concept of adding security features to a browser to prevent it from being used as a vector of attack to infecting a computer with malware. Such browser hardening techniques include:

Ad Block

Ad blockers are a significant first & foremost line of defense regarding the prevention of a security breach for systems that allow Internet access. Ads on the Internet are notorious for being vectors for Trojan viruses and browser hijackers that lead to more viruses, while other ads lead to malicious websites that masquerade as legitimate software companies whose software has been modified to contain a malware payload; this is known as malvertising. Ad delivery companies such as Google AdSense are also notorious for refusing to curate what ads they allow to be distributed through them and will platform anyone who pays for ad distribution through them without first vetting the client. For this reason, ad block is the first and foremost security measure any company that allows for Internet access should take regardless of what web browsers are being used. Recommended ad blockers are Ublock Origin or Ad Nauseam for standard CPU-based computers such as towers or laptops, and AdGuard for ARM-CPU systems such as smart phones and tablets. Ad block is also useful for keeping CPU lanes clear and RAM space empty so as to prevent wear and tear on the hardware itself. The Brave browser comes with ad block out of the box.

Decentraleyes

Decentraleyes is a browser add-on that provides localized JavaScript libraries that would ordinarily be provided by Google and prevents them from using their JavaScript from tracking end users and their behaviors.

Script Blockers & Tracker Blockers

Adblock by itself only goes so far in ensuring user privacy and security. Many websites have viruses or malicious script written into them by either hackers or the site owners themselves, and previously reliable and trustworthy websites fall from grace in this way, but may still prove necessary in their use. Therefore, it is apropos to make use of a script blocker such as Ghostery, NoScript, ScriptSafe or Avast Online Security to disable trackers and other malicious scripts. However, not all script blockers are made equal and the mileage of effectiveness between them may vary. Avast Online Security, for example, blocks trackers but not scripts. The Brave browser also comes equipped with script & tracker blocking features out of the box.

Miner Blockers

Browser miners work by using your CPU to crunch math for the purpose of minting new coins for cryptocurrencies, and while miners are themselves little more than a nuisance, they can push your CPU to its finite limits and prevent proper use of your computer. For this, minerBlock is recommended.

Web Reputation Extensions

Web reputation plugins for browsers are also another useful and effective security measure for Internet usage. Web reputation plugins inform the user what websites are secure to use and which sites are to be avoided. There are, however, disgraced web reputation plugins such as Web of Trust that were found to be collecting and selling user data. Avast Online Security is recommended in its place.

VirusTotal

VirusTotal is a website dedicated to letting users scan URLs and files for malware by scanning websites and files with every known and trusted anti-virus scanner to date. It also functions as a web reputation platform by allowing comments from end users and security researchers. An ounce of prevention is worth a pound of cure.

Archival Websites

Archival websites such as the Wayback Machine and Archive.Today are useful in not only saving existing websites from being forgotten once they go offline, but in Archive.Today's case, also in stripping out unwanted JavaScript from a web page to make it more secure for end-user viewing.

Proxies, VPNs & Tor

Proxy servers, virtual private networks and the Tor network all serve the same function but come with significantly different caveats. Their purpose is to enable browsing privacy to prevent websites from watching and logging your activity on the Internet by means of using someone else's IP address and in some cases, DNS configuration. This allows for a variety of security and access boons such as being able to access content that is either region blocked from your country to preventing others from spying on your network activity.

Proxy servers have to be accessed usually by plugging into it from a browser, and being a public server, proxies are notorious for being overused, low quality, low speed and constantly dropping service. Proxies, while typically free, are the least secure of the three since, while website owners can't identify you, the owner of the proxy can potentially be watching your activity instead and hold a greater degree of anonymity than you do.

VPNs are the modern go-to for people who seek to browse the Internet with privacy, security & high speed Internet. While this isn't the be-all, end-all of security, it is more stable and trustworthy than proxies. However, not all VPNs are made equally, some VPNs sell user data while others refuse to log user information, & in some cases the latter is even proven in court such as the case for Private Internet Access. Be sure to research your VPN service provider before using them to ensure that browsing activity cannot be spied on by either the websites being accessed or outside security breach attempts. The Tor network, however, is highly regarded as being the most secure of the three options, as it relays your data between a total of three servers before delivering content back to the user.

The Tor network is free to use but comes with the caveat that anybody can set up a Tor server and make themselves part of the network, including those with interest in corporate espionage such as competing companies or foreign governments. The Tor network is also notorious for sudden drops and slow Internet speeds due to operating on single core connections, so while ostensibly more secure than a VPN, the Tor network has a history of being unwieldy. A significant security risk in using Tor includes what are called exit nodes, which is the last server at the end of the server chain that fully decrypts the information before its received by the website the search request is directed at, and anyone operating an exit node can observe the information being sent over it, meaning that Tor is susceptible to phishing operations in which data is collected for the use of stealing information like user logins.

However, using Tor & a VPN together can help patch the security flaws of the exit node issue by creating an encrypted tunnel at every point of the connection, including the exit node itself.

DNS configuration

DNS stands for Domain Name System and is the system by which IP addresses & websites are associated together correctly. To locate a website, your browser needs the IP address of the website you're attempting to access, therefore when you search a website by name, your browser will send the DNS request to a recursive name server (RNS) that is operated by your Internet service provider (ISP) to match the requested website to an appropriate IP address. If the ISP's RNS doesn't have the matching IP address stored, it'll instead reference 13 different route servers that cater to top level domains such as .com or .net to find the matching IP address. These route servers have redundant servers around the world to ensure snappy and consistent delivery, and depending on where they're located and the connection speed leading to these servers, domain name delivery can take longer for some websites than others. Once the request has been received by the proper RNS, the server will then reference an authoritative name server (ANS) that contain a list of IP addresses and matching uniform resource locator (URL) which are all updated whenever someone purchases & registers a domain. Once the appropriate IP address has been retrieved, it's sent back to the RNS, then back to the user.

DNS requests are also a high profile target for hackers, if an RNS is breached, it can falsely return an IP address leading to a malicious website in association with the requested domain name rather than the real website. Many VPNs will provide DNS encryption or rerouting. However, if a VPN is out of the question, you can use public DNS servers such as the ones supplied by Google (8.8.8.8) and Cloudflare (1.1.1.1). Furthermore, switching over to these other DNS servers can enhance Internet speeds as well as encrypt Internet searches to further prevent man-in-the-middle attacks. However, configuring your DNS settings to another DNS server comes with the caveat of giving someone else your search term history in place of your ISP, so it is recommended to research the privacy policies of DNS server providers.

Internet Bonding

Internet bonding is the process by which packets are evenly sent through multiple different Internet connections. Sometimes this is done by having two separate Internet connections wired to a person's home from the same ISP for the purpose of creating a faster Internet service, but the act of bonding two or more Internet connections together creates the effect of sending a divided number of packets through different ISPs, meaning that a cohesive narrative of your activity can't be formed by monitoring only one of the connections you're using. Another upside of connection bonding is that it can significantly enhance the speed of your Internet connection the same way parallelization on a CPU with multi-threading enabled can make your software run with less friction.

Operating-System-Level Virtualization & Sandboxes

A virtual machine is an emulation of an operating system that can be ran entirely on the computer's RAM instead of its hard drive, ensuring that in theory, the virus infecting the dummy OS can't affect anything on the host machine. However, this is merely the ideal scenario and doesn't truly reflect reality. Even virtual machines have flaws, bugs & exploits that malware can key into so as to allow it to leak from the virtual machine into the host computer.

A second layer of containment is where sandboxes come in. Sandboxes are a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system. For a sandbox, Comodo is recommended.

Sandboxing a virtual machine to prevent a security leak into the host computer can be thought of as being similar to using VPNs together with Tor to ensure no raw data is being observed.

Router Configuration

If you have access to the router you're using, it's strongly recommended that you switch to the WPA2-PSK setting with the AES encryption. Routers also have firewalls in their firmware, make sure to block anonymous Internet requests by default as a minimum standard.

Filtering Platforms

Filtering platforms are programs that can manage which programs can communicate over the Internet. It's like the firewall on a router only installed on a computer to prevent applications from communicating out rather than an outside force trying to get in. One such program recommended for this purpose is Simplewall.

Anti-Virus Software

Anti-Virus software is a cornerstone of Internet browsing and exists for the purpose of blocking and/or removing malware from a computer. Anti-Virus software can range from being malware disguised as anti-virus software to greyware to legitimate anti-virus software.

While Windows Defender may be considered all that's necessary, your mileage may vary. Malwarebytes & their products are a mainstay of anti-virus software, but does not provide a firewall for free. Another recommendation is Avast Anti-Virus, which provides a free firewall. Another favored anti-virus is Bitdefender. No other anti-virus applications are recommended at this time.

Free and Open-Source Software

The free and open-source software movement is one started by the likes of Linus Torvalds and Richard Stallman. Free and open source software is software which is not only free to use but allows the end user to audit the code to investigate it for either flaws, vulnerabilities or malicious code, which is more secure than closed-source software, the contents of which are anonymous and can't be audited by the end user to check for security vulnerabilities or malice. Free and open source software is often hosted on code depots such as GitHub.

KeePassXC

KeePassXC is password management desktop software that functions as an encrypted ledger of usernames, websites and passwords and requires a master password to access one's ledger. KeePassXC offers additional layers of protection to end-users by providing the use of a YubiKey as a required step to gaining access to the ledger.

Linux Distros

90% of malware is designed specifically to target Microsoft Windows OS, therefore any given Linux distro is innately more secure than Windows by means of security-by-obscurity. However, Linux distros also sport a number of features which make it more secure than Windows, such as limited root access, firewalls, firmware verification and mandatory access control systems. Furthermore, Linux distros are by and large open source projects with thousands of voluntary contributors and due to this reason, anyone can audit the source code of a Linux distro for spotting errors and vulnerabilities to be patched. Most software made for Linux distros are free and open source, meaning the code base for all the programs for Linux operating systems can be audited and verified independently. There are also a number of Linux distros with unique security uses. However, unlike Windows, Linux distros do not have a large market share of antivirus software like Bitdefender, so user discretion is paramount to maintaining a secure system.

Linux Mint OS

Linux Mint is a Linux distro designed to mimic Windows to be user friendly to transitory users and is often a first choice for people new to Linux. It has its own app store for installing free and open source software, which helps control for Trojans. A Linux Mint distro installed to a flash drive is also useful for retrieving data off of dead SSDs and NVMes.

Tails OS

Tails OS is an amnesic operating system for using the Internet undetected, it comes with TOR installed and can only be ran off of a flash drive. Once that flash drive is pulled from the computer it's using, both the computer and the OS will completely forget what the end user was doing.

Qubes OS

The Qubes operating system designed around the concept of decentralized segmentation and is made up of a series of virtual machines controlled by a hypervisor that is designed to have disposable sandboxes that are meant to multi-boot an array of different operating systems that can be deleted on a whim and a new one spun in its place from said templates, so if one OS installed to a Qube is infiltrated with malware, it can't escape containment and the infected OS distro can be deleted and replaced by a fresh distro of like-kind. Qubes OS is often lauded as being the most secure operating system ever made.

Data Destruction

Finally we come to the final part of computer security, which is how to permanently destroy data that is no longer needed and can only pose a security risk by its persistence on a machine. When you delete a file from your computer, you're merely deleting a pointer to the data which represents your file, the data which makes up your file remains as unallocated space until it is selected to be overwritten by new data with its own pointer. However this overwriting process is unreliable, uncontrollable and may only yield a partial overwrite. This is where data destruction Linux distros are introduced. The purpose of a data destruction distro is to wipe a hard drive multiple times to ensure the data has been well and truly scrubbed. Such data destruction distros are as follows: Darik's Boot and Nuke, nwipe, Parted Magic, Shred with Linux Mint.

Compliance Officer: Bailey Campbell

970-476-5547
compliance@abiggerbettermortgage@gmail.com