DSCR PRO, LLC
730 17th St Ste 900
Denver, CO 80202

dscrpro@dscr.pro f-303-496-1800 o-970-476-5547 https://dscr.pro NMLS# 2712717

DSCR PRO, LLC

PRIVACY POLICY & INFORMATION SECURITY PROGRAM

Table of Contents

What is Privacy Policy and Security all About?

- Detecting, preventing and responding to attacks, intrusions, or other systems failures.
- Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Oversee service providers, by:
- Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
- Requiring your service providers by contract to implement and maintain such safeguards.
- Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

Basically, it’s about keeping consumer personal information safe and secure when sharing and retaining that information.

Initial Notice Requirement

§ 313.4 Initial privacy notice to consumers, code of regulations.

We are required to give consumers a copy of our privacy policy letting you know how your data will be used. If we sell your information, or shar your information. Our website publishes our company privacy policy and there is a permanent link on our company and emails that go out to consumers.

16 CFR 313.1 Requires a Financial Institution, in circumstances, to provide notice to you its privacy policies and practices.

Regarding IP Addresses

DSCR PRO, LLC, “DSCR PRO, LLC” or third parties use your IP address to identify you, gather broad demographic information, help diagnose problems with our server, and to administer our site.
Regarding Cookies. DSCR PRO, LLC. Third parties may be placing or reading "cookies" on your internet browser. Cookies are bits of text transferred to your computer hard drive through your browser. They allow DSCR PRO, LLC or third-party systems to recognize your browser, remember your information and link your activities to you. Should you block or disable these cookies, this site may not appear as intended. Nevertheless, if you want to take these steps, you can do so by following instructions related to your browser.

Cookies collect types of information such as the following:

- Site traffic EXAMPLE: the domain name and host from which you access the internet and the internet address of the site from which you came to ours
- Statistics EXAMPLE: the date and time you access our site, the keywords, links clicked, and the pages you visit
- IP information EXAMPLE: your computer's IP address, information about the operating system, platform and web browser type/version you utilize)

- Demographic information & other non-personally identifiable information about you
- Advertising information
- Information to fight fraud or misuse

Regarding Personally Identifiable Information

Some DSCR PRO, LLC sites may collect personally identifiable information when you choose to provide it through a contact form, registration form or when purchasing a service or product. This type of information may include your name, addresses, email addresses, phone numbers, and financial information. This information is used to contact you about an inquiry, to manage to promote our relationship with you. **We do not sell your information to any third party, though we do share your information with close and necessary third parties for the purpose of you loan request**. We do not give, share or sell your information to nonaffiliated third parties.

Selling and Sharing Your Information

We do not sell your information however, we do share your information with our vendors and wholesale lenders for underwriting and credit purposes when you apply for a mortgage or other financial service.

§ 313.14 Exceptions to notice and opt out requirements for processing and servicing transactions.
(a) ***Exceptions for processing transactions at consumer's request.*** The requirements for initial notice in § 313.4(a)(2), for the opt out in §§ 313.7 and 313.10, and for service providers and joint marketing in § 313.13 and do not apply if you disclose nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:
(1) Servicing or processing a financial product or service that a consumer requests or authorizes.
(2) Maintaining or servicing the consumer's account, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or
(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.

If you choose to OPT OUT from Advertising or Other

You may do so in writing by email to: DSCR PRO, LLC, 730 17th St Ste 900, Denver, CO 80202 or for faster results you may contact by email, optout@dscr.pro or you may call 720-722-3101

If you choose to opt out from necessary third party information sharing you must cancel your loan application as we must share your information to obtain financing for you.

Regarding Sensitive Information

Some DSCR PRO, LLC sites may, as part of your purchase of a product or service, collect sensitive information, such as your social security number, ID, address and birthday or credit card number. In such case, sensitive information will be encrypted and protected with SSL which current industry standard encryption protocol when you apply on the internet.

You will know you are on such an SSL page when you see a picture of a closed lock in the browser next to the company website domain name. Another way to tell if you are on a secure page is to look at the address or URL of the page. (Look in the address box or right-click on the page and select "Properties".) These secure SSL encrypted pages have URLs that start with https:// instead of http://.

Employees

Employees are required to have a secure password on their computers and have antivirus and malware on their computers. Employees also use private VPN which hides our online activity and location from hackers and internet service providers. This keeps our online privacy and your vital information secure.

Employee hiring procedure include a background check for all employees, including management, who are involved in the origination of mortgage loans against the U.S. General Services Administration (GSA) excluded Parties List, the HUD Limited Denial of Participation List (LDP List), and the Federal Housing Finance Agency (FHFA) Suspended Counterparty Program (SCP) List.

Regarding Information Collected by Third Parties

This site may consist of third-party advertising, links to other sites or content from third parties. DSCR PRO, LLC may share non-personally identifiable (for example: demographic) information to facilitate the delivery of relevant content advertisements. Third party sites, businesses, advertisers, or advertising entities working on their behalf, sometimes use technology to deliver the advertisements that appear on our website directly to your browser. They automatically receive your IP address when this happens. They may also use cookies, JavaScript, web beacons, and other technologies that they may use, and the information practices of these advertisers and third-party websites or businesses are not covered by this Privacy Policy but are covered by their respective privacy policies. Some, but not all, third party advertising companies provide a mechanism to opt-out of their technology. For more information and identification of advertisers that provide an opt-out mechanism, please visit the following: http://www.networkadvertising.org/managing/opt_out.asp

Regarding ownership and transfer of information

All information collected on this site is considered to be an asset of DSCR PRO, LLC and as such may be shared or transferred as described in this policy as part of an acquisition (or contemplated acquisition) from or to DSCR PRO, LLC or our site.

Regarding changes to this policy

DSCR PRO, LLC may alter this policy from time to time, so you are encouraged to review the policy periodically.

Legal Disclaimer

DSCR PRO, LLC may disclose personal information when required by law or in the good faith belief that such action is necessary to conform to the ethics of the law, or to comply with a legal process served on our Web site.

INFORMATION SECURITY PROGRAM & PROCEDURES

16 C.F.R. § 314.4 require and as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313, companies who keep records with personal information must implement, employee, office and computer securities to safeguard personal data, such as social security numbers, names, addresses and credit reports as to protect consumer’s financial information.

How we keep Your Information Safe

We keep your personal information on a secure server that has dual password protection. Your personal file is encrypted, and that password is kept secure on a different server. The second password is kept of a separate hard drive and kept in different locations. You must have access to all three to gain access. Those servers are also password protected and the server that keeps your retained records is not online and only holds records. It is not used for anything else. These are closed files that we are required to keep for up to seven years, after that they are permanently deleted from the hard drive unless we feel that further record retention is necessary.

Working files are only kept as a working file until it has resolution. That means it either funded and closed or was rejected either by the borrower or the lender. They are kept on hard drive are locked up in a secure location after hours so your information is not accessible from the working computer. Your information is never left on a computer so bypassing the password, which is not that hard, will not work because your information is not there. Our computers are equipped with two hard drives, one for files and one for the operating system. Employees using our computers at our office will only have access when they check in and employees never have access to our archive or close files.

Employee Training and Detecting Cyber Attacks

We have extensive training about information security and cyber attaches in our continued education, especially in 2025. Much information was covered in regards to keeping consumer records safe as well as our computers from getting a virus by opening a PDF document or an email that may have a virus or a reverse shell.

A reverse shell is when you allow another party access to your computer without knowing. It’s as if they are sitting at your desk and can access any of your files and software, change your passwords, create accounts or steel information. Using AdBlock helps keep virus and revers shell activity down. Ads can carry virus and clicking on it can open it or allow someone access to your computer without your knowledge.

Below are some suggested ways to help keep your computer from being hacked but the training doesn’t stop here. Sometimes it takes a human eye. We look at emails that we don’t recognize, such as a title company alerting us that our docs are ready to be viewed.

- Do you have a file open with that title company
- Is the email in the recognizable, normal format?
- Is there a file number, address and legal description on it, loan amount, etc.
- Is the email address from that company
- Does the email have company extensions or is it generic, look-a-like, or personal?

With the right training they are easy to spot. Some of these viruses or reveres shells are sent as a PDF, they have you as soon as you open it… don’t open it.

<u>Ad Block</u>

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.

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.

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:

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.

These are a few ways we and our employees keep cyber pirates out.

Who the Privacy Act Regulates and their Regulators

This part applies to those "financial institutions" and "other persons" over which the Federal Trade Commission ("Commission") has enforcement authority pursuant to Section 505(a)(7) of the Gramm-Leach-Bliley Act. An entity is a "financial institution" if its business is engaging in a financial activity as described in Section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates by reference activities enumerated by the Federal Reserve Board in 12 CFR 211.5(d) and 12 CFR 225.28.

The "financial institutions" subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under Section 505 of the Gramm-Leach-Bliley Act. More specifically, those entities include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that are not required to register with the Securities and Exchange Commission.

To learn more about privacy policies and our regulator, please visit https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-313/subpart-A/section-313.4

If you have further questions, please contact compliance:
compliance@abiggerbettermortgage.com
970-476-5547
Compliance Officer: Bailey Campbell