



---

## **Section 1 Privacy Policy Statement**

---

Maintaining the confidentiality, integrity, and safety of data generated, accessed, modified, transmitted, stored or used by Amherst Funding Group, L.P. (“AFG”) is a responsibility shared by all AFG employees.

AFG employees have the responsibility to protect AFG data from unauthorized generation, access, modification, storage, disclosure, or destruction. All AFG Employees are expected to be familiar with and comply with this policy. Violations of this policy can lead to disciplinary action including termination. Any known violations of this policy are to be reported to AFG’s Chief Operations Officer (“COO”).

## **Section 2 Reason For Having A Privacy Policy**

---

AFG recognizes the need to protect personal and confidential data which is generated, accessed, modified, transmitted, stored or used in connection with all aspects of our business model. All AFG employees have a responsibility to protect AFG data in all formats, including electronic, physical, and/or intellectual.

Nothing in this Privacy Policy is intended to serve as a restriction on the right of individual departments to require additional policies and/or procedures regarding any situation not addressed in this document.

## **Section 3 Data Management**

---

Data is a critical asset of AFG and as such requires protection from unauthorized generation, access, modification, disclosure, or destruction. Appropriate managerial, operational, physical and technical controls must be put in place within written policies and procedures that control access to, use of, and disposal of all confidential and personal information delivered to and utilized by AFG.

AFG will not trade, rent or sell any personal or confidential information to anyone. We will not provide account or personal information to non-AFG companies for the purpose of independent telemarketing or direct mail marketing of any products or services.

It is the responsibility of each individual with access to sensitive data resources, to use these resources in an appropriate manner and to comply with all applicable federal, state, and local statutes. Sensitive data is defined as any information that could cause an individual personal, financial harm if disclosed and used improperly. Additionally, it is the responsibility of each individual with access to sensitive data resources to safeguard these resources. Methods of safeguarding sensitive data include:

- Sensitive data should not be stored on personal desktop or laptop computers since these computers tend to reside in less secure locations than central servers.
- Access to computers that are logged into central servers storing sensitive data should be restricted (i.e. authenticated logins and screen savers, locked offices after normal work hours as well as on weekends and holidays, etc.)
- Access to sensitive data resources stored on central servers should be restricted to those individuals with an official need to access the data.



---

Additionally, such data will be encrypted at the data element level using 128bit Industry Standard Encryption.

- All servers containing sensitive data must be housed in a secure location and operated only by authorized personnel.
- Copies of sensitive data resources should be limited to as few central servers as possible.
- Sensitive data should be transmitted across the network in a secure manner (i.e., Strong Passwords, Secure Sockets Layer, 128bit Industry Standard Encryption, etc.)

## **Section 4 Electronic Data Disposal**

---

All computer systems, electronic devices and electronic media must be properly cleaned of sensitive data and software before being transferred outside of AFG's offices either as surplus property or as trash.

Computer hard drives must be sanitized by using software that is compliant with Department of Defense standards. Non-rewritable media, such as CDs or non-usable hard drives, must be physically destroyed.

The primary responsibility for sanitizing computer systems, electronic devices and media rests with the Technology Department of AFG.

## **Section 5 Who Needs To Know This Policy?**

---

All AFG employees who generate, access, modify, transmit, store, use or have access to confidential and/or personal data, as well as anyone who represent themselves as being connected, in one way or another, with AFG need to be aware of the contents of this policy.

AFG has arrangements with third-party vendors/companies whose experience and services are essential for our firm to operate with the highest levels of customer service and overall efficiencies. For example, we work with firms that perform complex pre-funding and post-funding quality control reviews and audits. Each AFG approved vendor/company performs their authorized functions at AFG's direction and we only share customer information that is necessary for them to perform the specific functions as defined by AFG. As with all our business partners, these companies are required to safeguard AFG information and only use it for authorized purposes, and within the guidelines established by AFG for the protection of customer information.

All third parties, including vendors, who have access to or control of AFG information described in this policy, must agree in writing to maintain such information confidentially and in accordance with all appropriate federal and state laws.

## **Section 6 Enforcement**

---

AFG's COO is charged with the promotion of security awareness within the firm as well as responsibility for the creation, maintenance, enforcement and design of training on relevant privacy standards to ensure the enforcement of AFG's Privacy Policy. The COO will receive, review and maintain reports of incidents, threats and malfunction that may have a security impact



---

on AFG's information systems. All incidents of actual or suspected security breaches must be reported immediately to the COO at 713.888.0086 or [bbrunner@amherstfunding.com](mailto:bbrunner@amherstfunding.com).

The COO is also responsible for maintaining detailed records of actions taken by AFG. The COO will conduct periodic audits to determine AFG is in compliance with this policy. The COO will investigate policy breaches and insure that appropriate corrective actions are taken, if needed. The COO will also respond to court ordered releases of information within the guidelines and constraints of both state and federal laws which govern these issues.

## **Section 7 Periodic Updates**

---

AFG's COO is responsible for updating, as well as tracking and publishing any new policies which are developed in response to any new state and federal laws and/or any incidents, threats or malfunctions brought to the COO's attention.