POLICY: OPERATIONS

Purpose: **Provide working guidelines for management and employees to follow ensuring compliance is not only consistent but within all state and federal regulations.**

Scope: **Define all company policies, nonhuman relations.**

These policies and procedures have been written in accordance with the Fair Debt Collection Practices Act and The Fair Credit Reporting Act. These Acts are attached here to in the appendix.

- **Nature of Operations**

The purpose of AAS Debt Recovery, Inc. is to provide debt collection services working as a third party. All clients sign a contract in compliance with Pennsylvania state law. All contracts are executed upon negotiated terms. All contracts maybe terminated with thirty days written notice. Contracts are updated accordingly with changing terms and laws.

2.0 Licensing

Licensing is received and updated for every state in which AAS Debt Recovery conducts business. Licensing is reviewed by AAS Management and/or Cornerstone Support to ensure compliance. AAS is currently licensed as a debt collector in the following states:
Pennsylvania
New Jersey
Florida
North Carolina
West Virginia
Maryland
Ohio

- **Site Security**

Physical security is maintained by passcode for access to the building. AAS operations are open from 8:00am to 5:00pm Monday thru Friday. After hours collections take place at management discretion. Offices are locked with alarms outside operation times. AAS servers and sensitive data storage are locked at all times within a separate data center. All critical papers or organizational documents are stored either in a fire proof safe that remains locked at all times or at an off-site storage facility.

4.0 Affiliates and Third-party Relationships

AAS Debt Recovery, Inc. is not affiliated with any other entities within debt collection or any financial institutions.

4.1 AAS Debt Recovery, Inc. uses the following service providers to perform routine activities.

- Credit Bureaus, Experian, Equifax and TransUnion (reporting only);
- UIS Support (data support), a privacy agreement is in place;
- FSN of Pittsburgh
- Horizon Debt Collection (v16, as of 6/4/2020), Horizon Support;
- Chex System (reporting only);
- Amixa (website maintenance);
- Billing Tree (credit card payments);
- USA epay Clear Payment Solutions (credit card payments);
- Comcast (ISP); and
- Cornerstone Support.

AAS Debt Recovery, Inc. reviews all service provider policies on a yearly basis for but not limited to compliance with federal consumer financial laws. An action plan is implemented should any problems be identified during the review. AAS may request on a yearly basis from its service providers policies, procedures, internal controls, and training materials if applicable.

5.0 Debt Ownership or Account Transfers

AAS Debt Recovery Inc. does not collect on purchased debt and does not purchase debt. AAS does not extend, renew or continue credit.

6.0 Internal Structure, Controls and Compliance Management

AAS Debt Recover, Inc. organizational chart identifies the responsibilities of key Managers.

- CEO

  Responsible for leading the development and execution of the company's long term strategy. Ultimately responsible for all day to day management decisions and for implementing long term and short term plans. Also, to ensure the company is appropriately organized and staffed and to have the authority to hire and terminate staff as needed. To authorize and ensure the annual budget is

maintained within approved expenditures. To ensure internal and external compliance and control measures are effective and monitored by the appropriate staff. To measure and control risk management of the company while always holding ethical guidelines to the highest of standards.

- President:

  Responsible for supervising the work of the other employees ensuring that they function together as an effective team. Helps to provide vision and sense of direction while scheduling and running the daily operations. Oversee that the direction of the strategic plan is completed while continuing to evaluate the success of the company. Maintains the competitive landscape improving new industry developments and standards.
    - Chief Financial Officer. Responsible for the direction and oversight of the daily financial postings. Ensures that payments are processed according to operational procedures and is directly responsible for the organizational cash flow. Creates and reconciles all GL accounts.
    - Information security manager. Responsible for the oversight of the information security program.

- Vice President:

    - Director of compliance. Develop, initiate, maintain and revise policies and procedures for the general operation of the compliance program. Reviews all compliance related topics. Responds to alleged violation of rules, regulations, policies, procedures by evaluating or recommending the initiation of investigative procedures. Develops and oversees a system for uniform handling of violations. Acts as an independent review to ensure compliance concerns are appropriately evaluated.
    - Client Relations Manager. Works to improve the company's relationship with current clients along with building relationships with potential clients.
- Collections Manager:

  Develops and administers collection programs. Oversees investigation of credit risk in customers and monitors the collection of amounts due. Designs and implements processes to improve cash flow. Manages collectors to ensure quality control. Handles collection issues at the point of contact. Oversees collection numbers, incoming calls, outgoing calls and makes changes to improve success. Ensures collection regulations are followed and updates collectors on changing environments. Instructs and trains collectors on technique.

- Council:

Responsible for representing AAS at all legal proceedings involving collections. Resolving and negotiating settlements. Oversight of legal action and court filings including executing judgments. Maintains applicable licensure and insurance.

6.1 Non-Management Positions

- Collections. Collectors are paid based on an hourly wage plus incentives. An incentive chart is reviewed and maintained by management.
- Legal. Paralegal staff is paid on an hourly wage plus incentives. An incentive chart is reviewed and maintained by management.

All positions include an incentive program. This commission structure varies for the type of position and tenure of the employee. Commission structures increase on either $5,000 or $10,000 increments based upon amount collected on a monthly basis.

While incentive pay is important to the organizational structure, AAS management performs routine spot checks using the daily payment history report to ensure accounts are updated and assigned correctly to avoid or eliminate any malfeasance. Any employee caught changing or manipulating the software system will be subject to corrective action or termination. Also, AAS operations primary exist for financial organizations and employee positions are determined based on prior banking experience.

7.0 Incoming and Outgoing Communications

As per the Fair Debt Collection Practices Act, AAS Debt Recovery Inc., ceases communication with consumers when a consumer refuses, in writing or by phone personally, to pay a debt or requests that the debt collector cease further communication, except to advise the consumer that:

- The collection effort is being stopped
- Certain specified remedies ordinarily invoked may be pursued or, if appropriate, that a specific remedy will be pursued
- Mailed notices from the consumer are official when they are received by the debt collector

All calls inbound and outbound by every staff member including management are recorded. Collectors must inform every incoming call is recorded. These recordings are kept on file for 5 (five) years. Calls are reviewed by management for quality assurance on a monthly basis or when a consumer has issued a complaint.

Collectors may only communicate via phone calls and specified, pre-approved letters that are relevant to the collection efforts. Collectors must adhere to only sending additional correspondence outside the mandatory 30-day dispute period noted in the response field in Collection Management.

Communicating with custom letters is prohibited. If it is necessary to customize communication due to an obscure situation, the letter must be approved by management or AAS attorney.

At no time is communicating with a consumer via e-mail permitted. AAS employees are forbidden to use any email communication to other employees or management outside of allowed email service implemented by IT services.

Communicating via fax is only permitted if the consumer assures it is their personal fax, and no one else will have access to the transmittal.

AAS Debt Recovery, Inc. does not use a predictive dialer for collection purposes.

Letters are reviewed and approved by an independent attorney every 2 years.

8.0 Leaving Voice Mail Messages

Collectors do not have to leave a voice mail message. Discretion should be used when deciding to leave a voice mail, especially to protect against third party disclosure. When leaving a voice mail for someone we have never communicated with always use the approved AAS Phone Script. A voice mail is never left if the collector is unsure of the number or it is a "generic" voice mail.

A voicemail is never left when the "generic" voicemail does not reverse back to the consumer, the number is unconfirmed and just states a last name such as "this is the Smith's", the source is from skip tracing, or the voice mail is a business that could be monitored by someone else.

Conversely a voice mail can be left if the message clearly states the consumer's name, the consumer gave the collector the phone number and we have spoken with that consumer recently, communication is ongoing with the consumer, or the consumer has requested a call back.

9.0 Using "Skip Tracing" software

For the sole purpose of locating customers all staff is permitted to use the IDI website. A username and password is required. Security is maintained by the website entity. This Website is to be used for business purposes only. Any employee using the website for non-business related purposes will be terminated immediately.

10.0 FDCPA/TCPA

Collectors are to follow the same phone script for every outgoing call:

Hello, we have an important message from AAS Debt Recovery reference # (AAS ACOUNT #). **The client account number is never communicated.**

Please call 1 (888) 829-0624 extension____.

Subsequent phone communications from collectors initiate with a reminder that the call is recorded and that all communication is from a debt collector. Collectors are able to create a surname to protect their identity however, misrepresentation of the company's identity or authorization is strictly prohibited. Collectors also may not make false statements regarding the purpose of the call and must always identify themselves as a bill collector. All letters and correspondence sent from the collectors is compliant with the outgoing communication section of this document, postcards are never used. Mailings to debtors are sent from AAS. Letters to debtors should never be sent by AAS Debt Recovery, Inc. to preserve the privacy of the debtor. All letters disclose that written communication is from a debt collector and any information obtained we be used for that purpose.

All charges to consumer debt are substantiated with the client and proper proof is provided with the file or upon request. AAS Debt Recovery, Inc. does not pursue litigation without complete documentation.

AAS Debt Recovery, Inc. business hours are 8:00 a.m. to 5:00 p.m. eastern time Monday - Friday. These hours are subject to change with management's approval. AAS Debt Recovery, Inc. policy follows federal guidelines. Calls are not permitted before 8:00 a.m. and not permitted after 9:00 p.m. Calls will be made between these hours and collectors are encouraged to vary hours and days that calls are placed to debtors as to not develop a calling pattern. AAS does NOT use auto dialer or predictive dialer software.

Only one call to a debtor per day is permitted unless the consumer has left a message or requested to be contacted.

Calls will be discontinued if a debtor specifically demands, in writing that calls are discontinued or the debtors work has a no phone call policy.
AAS Debt Recovery, Inc., has a zero tolerance policy against a collector engaging in harassing, oppressive or abusive conduct of any kind. If such conditions occur termination without further explanation is immediate.

AAS Debt Recovery, Inc., collectors never release account information without the debtors consent (also see information sensitivity policy). This consent can be done via the phone since all calls are recorded. Collectors are permitted to use pre disposed internet searches (skip trace) that are approved by AAS Debt Recovery, Inc. These websites are Accurint.com and Spokeo.com. Any other search engines must be approved prior to use. When a third party is contacted by a collector the phone script is as follows:

> Is (name) there? Is this a good number for (name)? If asked for any additional information collectors are only permitted to state they are calling from "AAS, and this is a personal business matter that I can only speak with (name)."

AAS Debt Recovery, Inc. does not communicate with debtors via email, or text messaging.

10.1 State No-Contact List

AAS Debt Recovery, Inc. maintains a copy of the NO CONTACT state list at all collectors work stations. This list is review and updated according every quarter. This list does NOT indicate the ability to perform collections in a certain region or state. AAS has the ability to collect accounts nationally.

The following states and cities do not permit contact via interstate communications. Do not mail or call them. If you **do not** see a state listed. You may contact the debtor by phone and mail. You may take payments from them.

Arizona
Arkansas
Buffalo, New York (AD)
Connecticut
District of Columbia
Hawaii
Idaho
Iowa
Kansas
Louisiana
Maine
Massachusetts
Nebraska
Nevada
New York City – which includes: Manhattan, Brooklyn, Queens, The Bronx and Staten Island
North Dakota
Tennessee
Utah
Washington (State)

11.0 Information Sensitivity Policy

AAS Debt Recovery, Inc. does not disclose nonpublic personal information about consumers to third party institutions for the purpose of information and marketing. AAS Debt Recovery, Inc. only provides nonpublic information to credit reporting agencies via secured web transmission. Data is electronically transmitted thru only Secure Transfer Protocol. Furthermore, AAS Debt Recovery Inc. is exempt from the Gramm-Leach Bliley Act as per said act, “The exception is permitted only if the financial institution provides notice of these arrangements and by contract prohibits the third party from disclosing or using the information for other than the specified purposes. A sample contract is attached in the appendix.

AAS performs certain cloud computing either via its secured payment website or our third party bill payment vendors or the credit reporting agencies. AAS only authorizes information transmissions thru encrypted and secured HTTP applications.

11.1 Consumer Files

All files delivered to AAS Debt Recovery Inc., are electronically uploaded into the secured system. Paper files are then either destroyed or not accepted. AAS Debt Recovery Inc., only works with clients who can provide a complete file for a consumer including but not limited to: Origination loan documents, payment history, and a consumer profile.

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of AAS without proper authorization.

The information covered 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).

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 AAS Confidential information (e.g., any confidential information should not be left unattended on desks or the conference room).

Questions about the proper classification of a specific piece of information, or about these guidelines in general, should be addressed to management.

All AAS information is categorized into two main classifications:

- Public
- Confidential

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 AAS.

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 client names and lists, consumer information, banking information, software information, company performance measures, and other information integral to the success of our company. Also included in Confidential is information that may seem less critical, such as phone directories, general corporate information, personnel information, etc.

A subset of Confidential information is "Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to AAS by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from accounts entrusted to AAS to client personnel contact information, to vendor lists, and supplier information. Information in this category is extremely sensitive. When it comes to any information about our clients or their clients, nothing is to be shared in any manner.

AAS Debt Recovery, Inc., personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact management for further guidance.

The Security Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the confidential information in question.

11.2 Minimal Sensitivity

General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "AAS Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "AAS Proprietary" or similar labels. Even if no marking is present, AAS Debt Recovery Inc., information is presumed to be "Confidential" unless expressly determined to be AAS Debt Recovery, Inc., Public information by AAS Debt Recovery, Inc., management.

Access: AAS employees, clients, contractors, people with a business need to know.
Distribution within AAS: Approved electronic mail and electronic file transmission methods are preferred.
Distribution outside of AAS internal mail: U.S. mail and other public or private carriers (FedEx or UPS), electronic mail and client electronic file transmission methods.
Electronic distribution: No restrictions except that it is sent to only approved recipients.
Storage: Keep from view of unauthorized people; do not leave in view on desktop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Shred outdated paper information; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

11.3 More Sensitive

Business, financial, technical, and most personnel information

Access: AAS Debt Recovery, Inc., employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within: Standard interoffice mail approved electronic mail and electronic file transmission methods.
Distribution outside of internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within, but should be encrypted or sent via a private link to approved recipients outside of premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

11.4 Most Sensitive

All Client data and their entrusted account information, trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company.

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Confidential information is very sensitive, you may should label the information "AAS Internal: Registered and Restricted", "AAS Confidential" or similar labels at the discretion of management. Once again, this type of Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (AAS employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution inside: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients. Using encryption is highly encouraged.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In shredder; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

12.0 Data Breach

Reference Pennsylvania legislative statute 73 Pa. State. ANN. 2301-2329. An entity that maintains, stores, or manages computerized data that includes PI or a vendor that maintains such data. Should a breach occur: an entity must provide notice of the breach if encrypted info is accessed and acquired in an un-encrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key. Does not include publicly available info that is lawfully made available to the general public from federal state or local government records. This applies only if unauthorized acquisition of computerized data materially compromises the security of a system. Allows telephonic notice of breach substitute notice allowed when cost of providing notice would exceed $100,000, affected class of individuals to be notified exceeds $175,000 or it the entity does not have sufficient contact info. Notification may be delayed if it will impede law enforcement investigation. CRA notified if 1,000 plus people to receive notice. All breaches should be reported immediately to AAS management.

12.1 Incident Response Plan

Should AAS incur a data breach the following will be instituted by management staff previously outlined. Staff will contact AAS President first, who will then coordinate the response. The IT consultant (UIS vendor) will be contacted. At the same time the AAS Vice President will contact the data breach insurance carrier who has 24/7 coverage. Axis the insurance carrier has partnered with Mullen Coughlin LLC, serving as AAS response council. An email will be sent to axiscapital.breachhotline@mullen.law and a phone call will be made to 844-445-6097. Mullen Coughlin LLC will then contact UIS and start to formulate a plan of response. Both will advise AAS of findings and conclusions. Should letters to clients need sent that will be done thru council's office. Should the authorities need to be informed that will also be done by council. Should a data forensic team need deployed council will hire and send. Most operations are covered under AAS's insurance policy.

13.0 Appropriate Measures

AAS Debt Recovery, Inc., computer use by anyone other than authorized personnel must be restricted so that, in the event of an attempt to access AAS corporate information, the amount of information at risk is minimized. To ensure access is restricted AAS Debt Recovery, Inc., uses TrustWave to scan possible vulnerabilities and policy violations. The scan is performed on a quarterly basis. In addition a business grade Sonic Wall prevents internal web site abuse while securing external ports preventing unauthorized access.

14.0 Configuration of AAS-to-other Business Connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary on an as needed basis.

15.0 Approved Electronic File Transmission Methods

File transmissions are done only via secured sites from approved vendors or clients. The use of Mozilla Fire Fox browser is encouraged.

16.0 Approved Electronic Mail

All email transmissions are in accordance with AAS information policy and collection policy. All emails containing personal information are sent using Edgewave encryption.

17.0 Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

18.0 General Information Technology

The information security manager is the President.

18.1 Digital information handled by employees

Electronic storage for files and reports are to be saved on the AAS server which is back-up daily at various times to a virtual server which includes one point-in-time cloud image backup. AAS prohibits storage on individual work stations. Transmission of data internally should be done via the AAS server. Electronic transmission of data outside AAS is done only by approved encrypted email. Data should always be completely expunged when no longer required. All external drives, devices, cell phones, removable media, CD, DVD, paper, etc. are not permitted to leave the office or be installed onto any work station except for express business permission from the information security manager for only approved devices. All un-needed paper is shredded by a business cross cut shredder. All equipment purchases (hardware and software) are made and approved by the information security manager exclusively. All expired equipment is destroyed at the direction of the CEO. Should an incident occur the security manager will promptly notify management and take appropriate actions to eliminate the incident..

18.2 System Controls

AAS uses Trustwave to perform an assessment and testing of system controls. Trustwave analyzes AAS servers for vulnerability and detects failures in security. This tool is executed on a quarterly basis or when deemed necessary by AAS management.

18.3 Security Program

All systems, programs, or software used by AAS employees are password protected. Passwords are at least 14 characters long and contain a capital letter, and a number or symbol. Currently this combination is considered un-hackable technology. Also, AAS uses a dual authentication system that ensures proper access to the system.

All network traffic is monitored for activity. Inbound traffic is denied access with the following exemptions:
Port 25 SMTP inbound email to exchange server
Port 443 HTTPS outlook web access and ActiveSync only to exchange server
Port 636 LDAPS allowed only from the IP block of edgewave email encrypted service
Port 4000 HTTP allowed inbound to only the phone system IP
Port 5004-5005 Generic TCP allowed inbound to only the phone system IP for voice
Port 5566-5567 Generic TCP allowed inbound to only the phone system IP for voice
Outbound Traffic is allowed except for:
Port 25 SMTP denied outbound for all machines except exchange server

Network security is monitored by a business grade Sonic Wall device (model TZ210).

All email that contains personal information is encrypted using TLS encryption to protect any emails that contain this sensitive information. The encryption uses Edgwave TLS communication server to server.

For response to an incident or breach see Section **12.1**

Data in transit is encrypted. Data at rest is also encrypted using software Bitlocker on AAS servers. AAS does not have any open ports listening on the outside of the fire wall and does not have exposure to the internet.

18.4 Disaster Recovery

AAS vendor (UIS) continuously monitors AAS server for continuity. A “keep alive” signal is sent to the vendor’s office every 2 minutes should 3 of these be missed a representative for UIS is alerted. UIS also gets notification alerts for active directory, IP addresses, and temperatures of server.

A hybrid backup approach with a local appliance as the first point for restores and virtualizations, and cloud storage for offsite redundancy and recovery as needed. Block-level backup technology that continuously tracks and stores incremental changes in data. Secure offsite cloud storage that automatically replicates data between tow geographically dispersed data centers. Advanced verification technology and multiple processes to test backups and ensure validity. End to end always encryption to continually protect data at rest and in transit. The backup frequency is every two hours twenty-four hours a day.

There are varying approaches to recovery that are dependent on the type of disaster, the different methods are as follows:

- Bare Metal Restore-Reformat the system from scratch and restore back to a physical or virtual system
- Local-Boot the system to a local virtual environment
- Cloud-Boot the system in the cloud
- Virtualize via Hypervisor-Export an image and boot the system to a virtual environment

Depending on the incident and potential impact, one or more to the following DR procedures will be activated.

- Missing File; Any missing file will be restored from the appliance to an alternative location
- Single Machine Corruption; A bare-metal restore to restore only the corrupted volume. If needed a virtualization of the machine will be done on the local appliance
- Single Machine Failure; virtualize the machine on the local appliance and connect to the network. Once the defective hardware is replaced, a bare metal restore without stopping the VM to test the recovery. After a successful test we will select an ideal date to execute the final bare-metal restore.
- Several Machines Down; virtualize the machines on a local appliance and connect to the network. The local appliance is not able to support the amount of VM's with reasonable performance a cloud virtualization process will be done. Once the local hardware has been repaired, we will select a date for recovery. The machines in the cloud must be stopped and recovery drives will be imported to the appliance to start the bare-metal restore.
- Site Down; Initiate a DR in the cloud. All desktops need to have a VPN client installed and running to connect these machines. Once the local site has been repaired, a date will be selected for recovery. The machines in the cloud will be stopped, and recovery drives with the latest backup will be shipped to the site. The drives will be imported to the appliance to start the bare-metal restore. This process will initiate downtime from the moment the VM's in the cloud stop and the bare-metal restore has been finished.

In the event of a disaster AAS will continue operations thru its complete back up restore outlined above. Estimated down time is ten (10) business days. AAS feels as though this amount of downtime is appropriate due to the nature of the business.

Since the core of our business is a traditional call center. Comcast would roll the complete phone system to an exterior location of determination or the phone system would be forwarded to outside lines if applicable. The estimated amount of time to accomplish this is included within our downtime policy.

18.5 Network Set up and Documentation

All Information Technology purchases are reviewed by the information security manager. Software contained on the server includes Horizon Debt collection V16, with a restricted number

of users, Quick Books, with a restricted number of users, IDI, with a restricted number of users and Windows 10 Professional, with a restricted number of users.

AAS has the discretion to secure certain information from employees. This is done on a case by case basis as needed to adhere to the information sensitivity policy.

18.6 Acceptable Use of Technology

All computers, fax machines, telephones, internet, email and voicemail are intended to be used to further business. None of these items are for personal use and disciplinary action may occur from misuse.

Due to the nature of our business the internet is not restricted or blocked from AAS employees. However, inappropriate use of the internet is strictly prohibited and certain search words will be blocked by AAS IT Service company and reported. Blocked search words will create a report provided to management.

18.7 IT Services

AAS utilizes the services of **UIS** for technology support, maintenance, planning and installation. **UIS** is responsible for these items.

19.0 Credit Report

Client, type of account, and balance determines outlined policy.

Non-Financial Institution services should not have a credit report, unless litigation is determined to be the source of collection.

Employees are trained regarding the use of consumer reports and management continues updates of training when necessary.
New accounts are to be entered in accordance to the FCRA in the following outlined matrix. The date of delinquency shall be the month and year of the commencement of the delinquency on the account that proceeded the action. Should that information should not be obtained then according to the FCRA the Rules of Construction will be followed.

- Report date will be the date the original creditor used.
- The original creditor will be asked what the DOD is.
- If these options are not available then a DOD will be derived by placement date.

Financial Institution services with balances under $1,500.00 need to be reviewed by management before a credit report is done.

Medical collections are not reported to the credit agencies until 180 days have passed from the delinquent date provided by the client. AAS will enter the account and place a hold on it until after the AAS-4 letter is sent.

Under no circumstances is collector able to "barter" with a debtor for payment if you remove their account from the credit bureaus. Once the account is reported, it stays in the bureaus. Paying off the account will update the bureau statuses to Paid.

The only way an account is removed from the bureaus is for one of the following reasons:

- Error by AAS Debt Recovery, Inc.;
- Error by Financial Institution Services;
- Client request;
- Proven Fraud or Identity Theft; and
- Management's approval.

Bartering is deemed to harm the integrity of the credit reporting process. The bureaus and ACA frown upon it. It is in our contracts with the bureaus not to make these deals with the debtors as doing so could jeopardize our ability to report.

Credit reporting for applicable clients is done twice per month usually on the 1st and 15th. Chex System Reporting is done on a weekly basis on every Wednesday. Should a holiday fall on a reporting day the reporting will be done either the next business day or the file will be submitted to the applicable agency for reporting the day prior to the holiday.

20.0 Direct Disputes (consumer complaints)

For purposes of this document a direct dispute means a dispute submitted directly to AAS Debt Recovery, Inc., by a consumer who is concerned with the accuracy of any information contained in a consumer report regarding an account that AAS Debt Recovery, Inc., has been assigned.

AAS Debt Recovery, Inc., as a general rule will conduct a reasonable investigation of a direct dispute if it relates to any of the following (in accordance with Regulation V):

- The consumer's liability for a credit account or other debt with AAS Debt Recovery, Inc., such as direct disputes relating to whether this is or has been identity theft or fraud against the consumer, whether there is individual or joint liability on an account, or whether the consumer is an authorized user of the credit account.

- The terms of the credit account or other debt with AAS Debt Recovery, Inc., such as direct disputes relating to the type of account, principal balance, scheduled payment amount on an account, or the amount of the credit limit on an open-end account.

- The consumer's performance or other conduct concerning an account or relationship with AAS Debt Recovery, Inc., such as direct disputes relating to the current payment

status, high balance, date of payment was made, the amount of payment made, or the date an account was opened or closed.

- Any other information contained in a consumer report regarding an account or other relationship with AAS Debt Recovery, Inc., that bears on the consumer's creditworthiness, credit standing, credit capacity, general reputation, personal characteristics, or mode of living.

20.1 Exceptions

AAS Debt Recovery will not conduct an investigation if the direct dispute relates to any of the following (in accordance with Regulation V):

- Any of the consumers identifying information such as name, DOB, SSN, telephone numbers, or address.
- Past or present employers.
- Requests for a consumer report.
- Any public record information such as judgments, bankruptcies, liens, and other legal matters
- Fraud alerts or active duty alerts
- AAS Debt Recovery, Inc., has reasonable belief that the direct dispute was provided by a credit repair organization.

20.2 Direct Dispute address and contents

All Direct Disputes are to be submitted to:
AAS Debt Recovery, Inc.
P.O. Box 129
Monroeville, PA 15146

AAS general email policy as described in the employee policies and procedures states the AAS does not communicate with customers via electronic mail.

The contents of a direct dispute must include the following (in accordance with Regulation V):

- Sufficient information to identify the account or other relationship that is in dispute, such as an account number and the name, address, and telephone number of the consumer, if applicable.
- The specific information that the consumer is disputing and an explanation of the basis for the dispute.
- All supporting documents or other information reasonably required by AAS Debt Recovery, Inc., to substantiate the basis of the dispute. This documentation may include, for example: a copy of the relevant portion of the consumer report that contains the

allegedly inaccurate information; a police report; a fraud or identity theft affidavit; a court order; or account statements.

20.3 Duty of AAS Debt Recovery, Inc.

Upon receipt of a direct dispute (in accordance with Regulation V):

- AAS Debt Recovery, Inc., will conduct a reasonable investigation with respect to the disputed information by obtaining written or verbal account verification from the original creditor.
- Review all relevant information provided by the consumer with the dispute notice and update the account via E-Oscar as in dispute. Send AAS Debt Recovery Inc., Client a validation request verifying the details of the debt and providing details for information provided by the consumer.
- Complete its investigation of the dispute and report the results of the investigation to the consumer before the 30 day expiration date beginning on the date that AAS Debt Recovery, Inc., received the direct dispute which is "time stamped" upon receipt via the below outlined data retention section.
- Should AAS Debt Recovery, Inc., determine upon receipt of the direct dispute that additional time is needed for its investigation it shall notify the consumer with 5 business days in accordance with the FCRA.

- If the investigation finds that the information reported was inaccurate, promptly notify each consumer reporting agency to which the furnisher provided inaccurate information of that determination and provide to the consumer reporting agency any correction to that information that is necessary to make the information provided by the furnisher accurate. This information is then validated with the client of AAS Debt Recovery, Inc. All notifications sent to the consumer from AAS Debt Recovery, Inc. are review and approved by an outside independent attorney who is authorized by the ACA.

AAS Debt Recovery Inc., logs and tracks disputes from consumers. A copy of this log is maintained and saved on AAS servers. A copy of this log is available for Clients review, upon request.

20.4 Data Retention

Upon receipt of direct dispute

- All direct disputes are logged into the AAS Debt Recovery, Inc., secure data base located on the AAS server. Please see internal policies relating to data security for additional information. At which time they are "stamped" by date.
- The data retention data base serves as a work flow device to ensure timely functions are performed. Applicable data base headings are used to direct said work flow. These headings include: Date Received, Manner Received, Account Number, Name, 30 day expiration date (based off date received), Nature of dispute, Client, Date to Client, Date

Returned, Clients Response, Action, Mailing Date, Manner Mailed, Documents Sent, and Additional Notes (which include any credit code updates).

20.5 Frivolous or irrelevant

Direct disputes will not be investigated by AAS Debt Recovery, Inc., if in fact AAS Debt Recovery, Inc., has reasonably determined that the dispute is frivolous or irrelevant (in accordance with Regulation V):

- The consumer did not provide sufficient information to investigate the disputed information as required.
- The direct dispute is substantially the same as a dispute previously submitted by or on behalf of the consumer, either directly to AAS Debt Recovery, Inc., or through a consumer reporting agency, with respect to which AAS Debt Recovery, Inc., has already satisfied the applicable requirements of the Act or this section; provided, however, that a direct dispute includes information listed above that had not previously been provided to AAS Debt Recovery, Inc.
- Upon making a determination that a dispute is frivolous or irrelevant, AAS Debt Recovery, Inc., must notify the consumer of the determination not later than 5 days after making the determination sent by mail.

- A notice of determination that a dispute is frivolous or irrelevant must include the reasons for such determination and identify any information required to investigate the disputed information, which notice may consist of a standardized form describing the general nature of such information.

Attached to this policy are AAS Debt Recovery, Inc., letters and correspondence to customers upon the receipt of a direct dispute. All dispute letters sent from AAS Debt Recovery, Inc., are reviewed and approved by the CNR attorney yearly.

This policy has been created following the guidelines of the Federal Regulations part 1022 FCR (Regulation V). AAS Debt Recovery, Inc., examines and updates internal policies on a quarterly basis.

20.6 Electronic Disputes E-OSCAR System/Chex Systems

Electronic disputes are handled in same directive as a written direct dispute. All disputes made via the E-Oscar system need to be investigated and concluded by the system generated response date within the E-Oscar program. When responding to the dispute the following procedures are maintained.

General Preparation

Log-in to the AAS Horizon system as well as E-Oscar. Once in E-Oscar select ACDV, ACDV WIP List. Choose the credit reporting agency. Take not of the response date. Copy the dispute

directly into the Horizon system as proof of receipt and to compare record information for accuracy.

CIF should be checked and updated accordingly. Last name, First name, Middle initial along with SSN, DOB and phone. Determine the associated CIF on joint accounts. Update the status code in the system to 93 and create the XB code for credit reporting using the information from the dispute as well as the CIF in Horizon. The images associated with the ACDV need to be saved and update the system notes with the dispute information.

Classification

The method of response is the same no matter of the dispute classification. For example when a dispute claims ID Fraud we validate with our client giving the dispute explanation. Should the client validate Fraud we delete and close the account. Documentation directly from the client is always used to make that determination. In addition in order for ID theft to be blocked by the CRA the customer must provide appropriate proof of the identity (or present suspicious documents or suspicious personal identifying information) and provide the CRA a copy of an ID theft report and a statement that transactions are not related to the customer. The customer's request must meet the criteria of the CRA to enable the block. AAS will work with applicable CRA's regarding ID theft.

Categories of red flags are used in accordance with CRA's. A flagged CRA or alert by the CRA fraud detection may induce a CRA marking of ID theft or Dispute placing that account on a hold until the CRA investigates.

Validation

Change the system R Code to 58 for a dispute. A validation request is then sent to the client. All paperwork is double checked in the file on Horizon to ensure it is valid. A list of client contacts can be found in the Horizon. The client response is also saved to the Horizon file for additional proof of debt. The E-Oscar dispute can then be updated with appropriate information and closed. An email is then sent to the assigned collector should additional follow up be needed.

Chex Systems

AAS does not receive direct disputes from consumers. When a financial institution that AAS reports on behalf of receives a dispute it is to be provided to AAS for investigation. AAS then investigates the dispute and updates the file accordingly for the weekly file submittal. The physical copy of the dispute response is then faxed back to ChexSystems 602-659-2910. A fax confirmation is then printed out by AAS to confirm transmission. A copy of that form is scanned into the appropriate AAS file.

Every Wednesday a batch file is created by the Horizon AAS system according to FIS protocols developed in 2020 at the direction of ChexSystems programmer (Adam Worzella). This file contains all updates from the previous file sent. This batch file is renamed to match FIS upload criteria (Chexaasdebt). The file is then uploaded into the "Inbound" folder on the FISDS secured

web portal. The file is automatically received by the FIS system. Should a system error occur AAS is to be notified of the error condition by the FIS team. This weekly file includes the following but is not limited to: NAME, ADDRESS, OPEN DATE, BALANCE, DELIQUENCY DATE, ACCOUNT NUMBER, and ACTION CODE of A, C or D. When a file has been paid, it will be updated on the following reporting Wednesday, partial payments are not reported per FIS system protocol.

21.0 Payment Process

AAS Debt Recovery, Inc. has the flexibility to accept payments in the following ways:

- Sending a personal check to our physical address or P.O. Box 129, Monroeville, Pa. See Payment negotiation for policy on personal checks.
- Credit Card by Visa, MasterCard, Discover, and American Express or check free of charge through our website at www.AASpayonline.com.
- Online at the company website.
- Payments made from consumers with multiple accounts will be split between accounts at the discretion of AAS.

When a consumer agrees to pay by a payment plan an authorization of that recurring payment is signed by the consumer.

AAS Debt Recovery Inc., does not accept payments by ATM's, Point-of-Sale terminals, automated clearinghouse systems, telephone bill-payment plans in which periodic or recurring transfers are contemplated, and remote banking programs.

Payments made to an account follow a simple payment matrix. The payment matrix is as follows: Interest, Fees, Debt, Legal Costs. The debt amount is provided directly from the Client of AAS Debt Recovery, Inc. When an account has been paid in full a PIF letter will be generated upon request.

Payments received by the office either electronically or physically are posted within two business days. All payments posted for a particular day are reflected to the account via an overnight process. Once a payment is posted it is delivered to ASS Debt Recovery's financial institution the same day.

NSF will be reported to the consumer by written letter notice and system notes will be updated accordingly.

If a consumer owes several debts that are being collected by the same debt collector, payments must be applied according to the consumer's instructions.

22.0 Payment Negotiation

Personal checks are accepted as payment. However, once a debtor has had funds returned on more than two occasions the debtor will then be required to make payments by certified funds only. No written notice is issued to the debtor when this policy is broken, only telephone communication.

AAS has clients that are willing to settle accounts for a percentage of the original owed. This is upon contractual basis and outlined during intake.

23.0 Clean Desk/Office Policy

An effective clean desk/office effort involving the participation and support of all AAS employees can greatly protect paper documents that contain sensitive information about our clients, customers and vendors. All employees should familiarize themselves with and practice the guidelines of this policy.

The main reasons for a clean desk and office policy are:

A clean desk/office can produce a positive image for visitors and as well as personal.
It reduces the threat of a security incident as confidential information will be locked away when unattended. Sensitive documents left in the open can be stolen by a malicious entity.

Scope

- At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in your drawers.
- At the end of the working day the employee is expected to tidy their desk and to put away all office papers. AAS provides locking desks and filing cabinets for this purpose.

Action

- Allocate time in your calendar to clear away your paperwork.
- Always clear your workspace before leaving for longer periods of time.
- If in doubt - throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the shredder.
- Consider scanning paper items and filing them electronically in your workstation.
- Shred sensitive documents when they are no longer needed.
- Lock away portable computing devices such as laptops or PDA devices
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

24.0 Time Barred Debt

As per the AAS Debt Recovery Inc., standard contract AAS does not accept nor does it pursue collections on time-barred debt. Should an account be received by AAS that exceeds the statute of limitations AAS will not pursue litigation marking the file accordingly and advising the client.

25.0 Repossession

AAS Debt Recovery, Inc. does not repossess or threaten to repossess property through judicial action. All received property is conducted via a sheriff sale in accordance with state and local law. Management attends sheriff sales and maintains a PA (state) Collector/Repossess license. A copy of this license is on display in the office.

26.0 Litigation Practices

Before any litigation proceeds to formal filing it is accepted and reviewed by AAS Debt Recovery's in house attorney and approved in writing by the client.

Before any file is sent for review by the attorney it is reviewed by AAS Management to ensure quality assurance. As part of the internal review process a check list is performed for each account entering litigation. This includes reviewing credit reports, property reports, phone call logs and the Service members Civil Relief Act (SCRA). A copy of the negative SCRA must be included in the file in order to file suit. Please refer to the Dinsmore fact sheet for additional information.

After a file has been assigned to the legal staff it is under the direct purview of our in house attorney. All litigation is closely followed and within state and federal guidelines.

27.0 Employee Training

AAS Debt Recovery, Inc. is a member of the American Collection Association (ACA). AAS participates in training offered by the ACA as well as compliance education.

27.1 New hire training

AAS ensures all staff has relevant knowledge, skills and expertise to perform work consistently high standards to achieve full potential. All new hires are subject to background and credit checks performed by the Information Security Manager (CEO). Security clearances are not required. Any and all negative discoveries determined result in disqualification of employment and may result in employment termination if discovered post hire. Since the natural of AAS business is financial institutions a preference is given to those potential hires however, all applicable background checks still apply.

The senior collector is responsible for training new employees on AAS software as well as "skip tracing" techniques. Phone scripts are provide to new employees to ensure proper phone technique. All calls are recorded and occasionally are monitored by management for quality assurance. AAS IT servicer sets up new users for access to the internal network and email if applicable. Management documents the new user for access to Horizon (collection software). A new user is created, all users are created with the same access accept for certain members of management. Any account change must be approved by management. No, accounts on the system can be deleted without management approval code.

27.2 Persistent employee training

Continual training for employees and management are provided by the ACA who AAS is a member of. Website and conference training are available thru the ACA website. Management is encouraged to attend and include staff on available training resources. Meetings are held to inform staff about policies, potential issues, safe practices and changing collection laws. Material containing new training techniques is circulated for review and discussed as appropriate.

TABLE OF CONTENTS

- Appropriate Measures
- Configuration of AAS-to-other business connections
- Approved Electronic File Transmission Methods
- Approved Electronic Mail
- Company information system resources
- General Information Technology
- Credit Report
- Direct Disputes
- Payment Process
- Payment negotiation
- Clean Desk/Office Policy
- Time Barred Debt
- Repossession
- Litigation Practices
- Employee Training