FINANCIAL SERVICES COMPLIANT ACCREDITATION PROGRAM APPLICATION

General Instructions for FSC accreditation approval: Applicant is a NAPPS member in good standing. Applicant maintains through this application that all policies and certificates are current. Applicant further acknowledges that policies are reviewed periodically, and changes are communicated and documented. Complete application and submit with requested documentation to: FSC@NAPPS.ORG. **Please allow 4-6 weeks for committee review**.

Date:

Name of the Participant Company:

NAPPS Member(s) Name(s): Please list all NAPPS Members associated with Company. Include name, email and phone contact information for each member:

Does the Participant Company own, or employed by or otherwise controlled by another company or other entity? No If yes, provide the company/entity name and address:

Participant company corporate address:

Participant Company's additional office location(s): Include address, city and state as it appears on the NAPPS website:

Participant Company website address:

List all company service offerings:

Please indicate if Company, Affiliates or Principal member has been subject to an investigation by governmental entity within the last 12 months. No If yes, explain:

List any and all Judgments: (Include case caption to include jurisdiction information) against Company or Affiliates, rendered for services related to: Foreclosure, Collections, and or the Sale and Marketing of Real Estate within the last 10 years. Please indicate "na" if not applicable

The following policies, procedures and certificates are MANDATORY for acceptance into the NAPPS FSC Accreditation

Corporate Infrastructure Must demonstrate all business licenses required in each state of operation and demonstrate that employees and vendors are well versed in company policies and procedures.

1. Certificate of Business Insurance
2. Certificate of Business License and State Legal Entity Registration
3. Code of Conduct Policy for Employees
4. Description of Case Management Software (CMS) *Software must possess the ability to protect personal data, restore in the event of disaster recovery, and audit service results of process service network*
5. Disaster Recovery plan *Must include how often the plan is updated and tested; outline of alternate location to conduct business if primary office is compromised; Disaster Recovery policy of 3rd party software vendor if applicable*
6. Vendor Management Policy *Must outline and demonstrate the organizations ability to effectively manage vendors to include organizations primary process server network and must contain all of the following components: Outline of onboarding process for new vendors and contractors, Confidentiality Agreement, Contractor Service Level Agreement, Code of Conduct for Contractor.*
7. Visitor Sign In Policy *Must include appropriate use of wi-fi network and guest password.*
8. Document Retention and Destruction policy

Information Security Policy Must demonstrate organization ability to define and monitor security controls. Policies must be communicated, enforced, and audited to be effective.

1. Information Security Policy *Must include how often policy is reviewed and updated*
2. User Access Policy *Must outline how authorized users gain access to computers. Include a Remote Access Policy if application includes branch offices or home office users accessing the company network remotely.*
3. Password Policy *Computers in office and Case Management Software (if separate)*
4. Third Party Access Control Policy (if applicable) *Must outline formal procedures for third-party access to company owned network and applications.*
5. Mobile Computer Policy *Must define how sensitive data is password protected to secure any confidential data that may be stored on the computer.*
6. Removable Media Policy *Must define principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.*
7. Wireless Use Policy *Must define the use of wireless devises and protects the organizations resources against intrusion*
8. Anti-Virus Policy *Must define anti-virus programs on every computer including how often a virus scan is performed; how often is it updated; what programs will be used to detect, prevent, and remove malware programs; what type of file attachments are blocked at the mail server; what anti-virus program will run on the mail server; and how anti-spam firewall will be used to provide additional protection to the mail server.*
9. Data Management Policy *Must define how data is stored, backed up and encrypted within network and Case management system.*
10. Incident Response Plan *Must define the response to a security incident such as a virus, network intrusion, abuse of a computer system or other situation.*

RECOMMENDED: The policies listed below are recommended for an organization's continued demonstration of solid business practices but are not required to obtain FSC accreditation.

- Employee Handbook
- Document Shredder Service: Removes documents offsite with secure shredding process.
- Service Level Agreements with Clients and Vendors
- Clean Desk Policy
- Employee Criminal Background and drug testing
- Contractor Management *Demonstrate that Driving Records and Criminal Background Checks are routinely conducted on Primary Process Server Network*

By Signing this agreement participant acknowledges that the information contained herein is accurate and all policies will be maintained in accordance with NAPPS FSC accreditation guidelines.

Company Name: Signature:_____

Print Name: Title: