OP.300: Information Technology– AgCountry, FCSAmerica & Frontier

On 07-24-2024 the Board of Directors of AgCountry Farm Credit Services, ACA, sitting for itself and concurrently as the Board of Directors of its wholly owned subsidiaries, AgCountry Farm Credit, FLCA and AgCountry Farm Credit, PCA, (hereafter, collectively "AgCountry Board") adopted this policy; the Board of Directors of Farm Credit Services of America, ACA, sitting for itself and concurrently as the Board of Directors of its wholly owned subsidiaries, Farm Credit Services of America, FLCA and Farm Credit Services of America, PCA (hereafter, collectively "FCSAmerica Board") adopted this policy; and the Board of Directors of Frontier Farm Credit, ACA, sitting for itself and concurrently as the Board of Directors of its wholly owned subsidiaries, Frontier Farm Credit, FLCA and Frontier Farm Credit, PCA (hereafter, collectively "Frontier Board") adopted this policy.

Objective

The objective of this policy is to ensure:

- information technology is utilized effectively and appropriately to provide the best possible service to Employees, Directors and Customers, supports Association operations, and meets the objectives of the Association's strategic and business plans; and
- appropriate safeguards and controls are established and maintained for Association, Customer, Applicant and Employee information.

Source References

This policy sets out the expectations for compliance with Farm Credit Administration ("FCA") Regulations §§609.905 - 609.950, FCA policy Statement FCA-PS-77, FCA Bookletter BL-069, and FCA Informational Memoranda ("IMs") dated 08-30-1999 (Threats to Information Management Systems), 12-16-2014 (Cybersecurity Framework and Other Recent Guidance), 08-05-2015 (Cybersecurity Assessment and Expectations for System Institutions), and 06-27-2017 (Business Reporting and Continuity Security).

Operating Parameters

Definitions

Following are the definitions of various terms used in this policy.

- **Agent:** Any Person, other than a Director or Employee, with the power to act for the Association either by contract or apparent authority and who currently either represents the Association in contacts with third parties or provides professional or fiduciary services to the Association.
- **Applicant:** Any Person that has made application for extension of credit, an application for restructuring or requested a related service from the

Association, but has not yet entered into a loan, restructuring or service contract or other legal instrument with the Association.

- **Association**: AgCountry Farm Credit Services, ACA, and its wholly owned subsidiaries (AgCountry Farm Credit Services, FLCA and AgCountry Farm Credit Services, PCA), Farm Credit Services of America, ACA, and its wholly owned subsidiaries (Farm Credit Services of America, FLCA and Farm Credit Services of America, PCA), or Frontier Farm Credit, ACA, and its wholly owned subsidiaries (Frontier Farm Credit, FLCA and Frontier Farm Credit, PCA).
- **Association-Provided Information Systems and Equipment:** The servers, personal computers, laptops, notepads, telephone or cellular telephone technology and any software installed or services used in connection with on such hardware, including but not limited to e-mail, instant messaging, text messaging, and voice messaging provided to or otherwise made available to Employees and Directors to conduct Association business or for personal development as authorized by the Association.
- **Customer (or Member):** Any Person who has borrowed funds or received other services from the Association for which the Association receives interest, fees or other compensation pursuant to a loan or lease agreement, contract, or other legal instrument.
- **Director**: Any Member of the Association Board.
- **Electronic Business**: Refers to buying, selling, producing, communicating or working in an electronic medium.
- **Employee:** Any full-time, part-time, or temporary employee of the Association.
- **Entity (or Legal Entity):** A corporation, company, association, firm, joint venture, general or limited partnership, limited liability partnership, limited liability limited partnership, limited liability company, society, joint stock company, trust (business or otherwise), fund, or other organization or institution, whether de jure or de facto, no matter how denominated, except System Institutions.
- **Person:** An individual or an Entity.
- **System Institution:** Any bank, association or service corporation chartered under the Act, the Federal Farm Credit Banks Funding Corporation, and any other Entity statutorily designated from time to time as a System Institution and regulated by the FCA. It does not include the Federal Agricultural Mortgage Corporation.
- **Third Party Service Provider**: Any Person providing goods or services to the Association for a price pursuant to an agreement or contract, but who is not under the direct control of the Association and does not otherwise qualify as a Director or Employee. This term may include a Person (e.g., Agents) with access to confidential or sensitive information or who has an ongoing relationship with the Association. The following are examples of Third-Party Service Providers: information technology service providers, real estate appraisers, attorneys, and accountants.

Use of Association-Provided Information Systems and Equipment

Employees, Directors, Agents and Third Party Service Providers will use Association-Provided Information Systems and Equipment for authorized Association-business purposes or professional development and education. Limited personal use will be permitted if it does not interfere with the ability of the Association to conduct Association business or with an individual's devotion of duty obligation.

Employees, Directors, Agents and Third Party Service Providers shall use Association-Provided Information Systems and Equipment in compliance with all Association policies, standards, procedures and guidelines. Employees, Directors, Agents, and Third Party Service Providers shall have no rights or expectations of privacy covering any and all data, material or any other files stored or created on Association-Provided Information Systems and Equipment, or their internet usage when using Association-Provided Information Systems and Equipment. Failure to comply with this policy may result in disciplinary actions, up to and including for an Employee, termination of employment, for a Director, removal from the Association Board, and for Agents and Third Party Service Providers, termination of a contract.

Information Technology

The Association’s technology teams ensure information technology is utilized effectively and appropriately to provide the best possible service to Employees, Directors and Customers, supports Association operations, and meets the objectives of the Association's strategic and business plans. To meet these objectives:

- The Association will annually forecast the information technology services, hardware, software, communications, and personnel requirements as they relate to the Association’s strategic and business plans and incorporate the forecast into the Association’s Technology Plan. To maintain agility and best meet Association objectives, the technology teams follow agile product life-cycle practices for work intake, prioritization, and execution. Work is completed based upon prioritization and may not always follow the forecast as documented in the annual Technology Plan.
- Unless otherwise expressly provided, the Association shall be deemed the sole owner of any and all data, material or any other files (excluding any illegal material) stored or created on Association-Provided Information Systems and Equipment. This ownership is subject to and governed by the Association’s policies F.402 Data Privacy Policy and F.403 Data Management. The data privacy policy outlines the standards and practices for ensuring the confidentiality, integrity, and availability of data, addressing compliance with applicable privacy laws and regulations. Employees, Directors, Agents and Third Party Service Providers shall have no rights or expectations of privacy covering any and all data, material or

any other files stored or created on Association-Provided Information Systems and Equipment, or their internet usage when using Association-Provided Information Systems and Equipment.

- The Association recognizes the importance of maintaining the security and efficiency of key business systems by consistently installing current software releases and updates. This commitment extends to implementing regular software updates and conducting monthly patching to address security vulnerabilities and enhance system performance. Our approach to vulnerability management is proactive and systematic, ensuring that potential security weaknesses are identified and remediated promptly. All these activities are conducted in strict adherence to Policy OP.302 Security, which outlines the procedures and responsibilities for safeguarding our digital infrastructure against cyber threats. This policy underpins our dedication to protecting the Association's data and systems from unauthorized access, ensuring the integrity, confidentiality, and availability of our information assets. Only approved software may be loaded onto any Association-Provided Information Systems and Equipment.
- The Association reserves the right to audit, monitor, test, and conduct periodic reviews of Employee, Director, Agent and Third Party Service Provider compliance with Association policies, procedures and standards.

Disaster Recovery & Business Continuity

The Association have a comprehensive business continuity plan which includes information technology disaster recovery activities and plans. These plans are designed to ensure the recovery and integrity of the critical data, guarantee the continuation of essential business operations, and minimize service disruptions in the event of unforeseen incidents.

Specific measures include maintaining up-to-date backups of all vital data, utilizing redundant systems to ensure business operations can continue seamlessly, and implementing robust processes to restore information technology services swiftly and efficiently. Moreover, these plans encompass detailed protocols for communication and coordination among different departments, ensuring a cohesive and effective response during a crisis.

To validate and enhance the effectiveness of these strategies, the Association commits to conducting rigorous annual testing of both the technology disaster recovery and business continuity plans. These tests will be comprehensive, involving scenarios that simulate various types of potential disruptions. The insights gained from these exercises will be used to refine and update the plans, ensuring they remain robust and responsive to evolving threats and business needs. All activities and updates related to disaster recovery and business continuity will be documented and reviewed in alignment with the Association's overall risk management framework.

Vendor Management Program

The Association maintains a robust vendor management program for Third Party Service Providers. This includes appropriate risk mitigation controls,

and management of Third Party Service Providers. To meet these objectives, the Association will follow the requirements of the established vendor management practices and shall complete appropriate due diligence with respect to any prospective information technology or application Third Party Service Provider.

Association Employees will follow the requirements of the established vendor management practices and shall complete appropriate due diligence with respect to any prospective information technology or application Third Party Service Provider.

Information Technology Assets

Major hardware, network, and software purchases or development will be included in the Technology Plan, Security Plan and annual budget. At the time of a major acquisition and throughout the solution life cycle, the vendor management program requirements will be followed. Acquisitions will be approved by inclusion in the annual budget; approval of the budget constitutes approval of the acquisitions. All Association hardware and software must be procured through established technology practices.

The Association maintains a corporate-wide inventory of the Association technology assets. Ownership shall be assigned to Association's major technology assets. All persons entrusted with the Association property are responsible for its proper use, care, custody, and safekeeping.

All Association-Provided Information Systems and Equipment used to store, process or transmit Association information must have an attached, unique identifier (e.g., internally assigned asset tag or use the vendor serial number) to facilitate performance of physical inventories.

The Association shall maintain perpetual inventory control for Association-Provided Information Systems and Equipment, including a record of location and equipment owner for all equipment re-issued to others, as well as physical security over equipment currently in possession by technology.

The disposition of excess and obsolete hardware and software will comply with the requirements of Policy OP.401: Real and Personal Property Management.

Delegated Authorities

Association leadership is hereby delegated authority to:

- develop and implement standards, procedures and guidelines (including appropriate training) for compliance with this policy;
- monitor and evaluate compliance with this policy;
- take appropriate action to correct deviations from this policy; and
- approve exceptions to this policy, when such exceptions are essential to the effective administration of Association operations and are not prohibited by statutes, regulations, charters or bylaws.

The Association Board reserves the right to:

- revise or withdraw delegated authorities at any time; and
- develop, amend, or repeal this policy at any time.

Internal Controls

Association leadership will develop and implement appropriate internal control procedures to monitor compliance with this policy. These internal controls will provide reasonable assurance that policy requirements are met, deviations from policy requirements are detected, exceptions are identified and reported, and corrective actions are taken to restore compliance.

Reporting Requirements

To the greatest extent possible, policy reporting shall be completed through joint meetings of the Association Boards, joint meetings of the Association Board Committees (Audit, Business Risk, Governance or Human Capital) or the Joint Executive Committee of the Association Boards.

Association leadership will provide the Board:

- An annual assessment of the Association's technological environment and capabilities;
- An annual review of the business continuity and disaster recovery test efforts and plans;
- Quarterly progress reports concerning the Association's Technology Plan activities;
- Quarterly updates on key performance and risk metrics; and
- Quarterly updates on Third-Party Service Provider risks including vendors with high-risk security or financial posture, Service Organizational Control (SOC) report compliance or SOC control deficiency exceptions, regulatory compliance risks, or service level agreement uptime deficiencies.

Exception Procedures

All exceptions granted by Association leadership under this policy and all unauthorized exceptions to this policy identified by Association leadership must be promptly reported to the Association Board. Such reports will be made at the next regularly scheduled meeting of the Association Board unless:

- the exceptions result in risk or cost to the Association that warrants immediate reporting; or
- the granting or discovery of the exception does not permit enough time to reasonably prepare reports before the meeting and the cost and risk to the Association warrant delay until the next scheduled meeting.