OP.302: Security – AgCountry, FCSAmerica & Frontier

On 04-17-2024 (effective 04-15-2024) 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 effective management and security practices to:

- Prevent unauthorized access or use of confidential or sensitive Association, Customer, Applicant, Director and Employee information;
- Provide adequate controls to safeguard the Association's reputation and ongoing operations; and
- Support the objectives of the Association's strategic and supporting business plans.

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 dated 08-30-1999 (Threats to Information Management Systems), 12-16-2014 (Cyber Security Framework and Other Recent Guidance), 08-05-2015 (Cyber Security 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.
- **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.

Security Plan

The Association will enhance its technological capabilities, strengthen its security posture, and align cyber risk management initiatives with business objectives to support sustained growth and resilience.

- Annually, the Association Board will review and approve a Security Plan, which will adhere to industry standards to uphold the Association's safety, soundness, and regulatory compliance.
- The Security Plan will outline specific objectives, performance metrics, and goals to guide its security related initiatives and investments based on factors likely to impact the Association. This includes emerging threats, innovative technology solutions, and regulatory changes.
- Association leadership will annually forecast the security budget and resource requirements as they relate to the Association's strategic and supporting business plans and incorporate the forecast into the Security Plan.
- An itemized overview of the security budget will be available to support the Security Plan initiatives to reflect planned expenditures and allocations.
- The Security Plan will assess the maturity of its cyber risk management capabilities, including proposed initiatives, to ensure alignment with the Association's objectives and industry standards while mitigating risk.

Cyber Risk Management

The Association will maintain appropriate cyber risk management practices to ensure safety and soundness of its operations. Association leadership will identify, assess, implement, maintain, and document effective strategies and controls to mitigate cyber risks. Association leadership will

- Conduct an annual cyber risk assessment encompassing both internal and external factors likely to impact the institution. The risk assessment will identify and evaluate internal and external factors that may lead to unauthorized disclosure, misuse, alteration, or destruction of confidential or sensitive information, as well as Association-Provided Information Systems and Equipment.
- Ensure the effectiveness of resilient internal controls by conducting periodic testing and independent assessments of key controls, systems, and procedures of the cyber risk management practices, as deemed appropriate by Association leadership. Material deficiencies identified will be addressed promptly.
- Incorporate security risk within its comprehensive enterprise risk assessment framework.
- Association leadership will follow the standards for security as established by the FCA. Those standards are based upon the National Institute of Standards and Technology guidance.

The Association acknowledges the fundamental principles of confidentiality, integrity, and accountability as key components of an effective security

policy in compliance with Policy F.402: Data Privacy and Policy OP.301: Enterprise Content Management.

The Association has the right to inspect information stored on any Association-Provided Information Systems and Equipment at any time.

Association Employees, Directors, Agents, and Third Party Service Providers are responsible for maintaining and safeguarding Association data, including sensitive or confidential Director, Employee Customer, or Applicant, information stored on Association-Provided Information Systems and Equipment.

Vulnerability Management

The Association's vulnerability management practices will proactively identify, assess, prioritize, and mitigate security vulnerabilities across the Association's network, systems, and applications. Through continual monitoring for potential weaknesses and implementing timely remediation measures, these practices will reduce the Association's exposure to cyber threats and minimize the likelihood and impact of adverse security events. Additionally, it seeks to enhance the resilience and security posture of the Association, safeguard confidential or sensitive information, and maintain compliance with regulatory requirements and industry standards. Ultimately, vulnerability management practices support the Association's mission by fostering a culture of proactive risk management and ensuring the integrity, availability, and confidentiality of its digital assets.

- The Association will utilize a risk-based approach to enhancing its resilience by identifying and prioritizing potential threats and vulnerabilities based on an analysis of inherent versus residual risk.
- A defense-in-depth strategy will be implemented, comprising multiple layers of complimentary security controls. These layers will work collaboratively to provide comprehensive protection against cyber threats.
- The Association will implement measures to protect against reasonably anticipated cyber threats or hazards that may compromise the security or integrity of confidential or sensitive information. Additionally, the Association will enact protocols to prevent unauthorized access to or use of said information.
- The vulnerability management practices will be designed to assess the Association's digital environment on a regular cadence, prioritize vulnerabilities based on severity, and implement timely remediation measures to minimize the risk of exposure or exploitation.
- As part of the Association's vulnerability management practices, threat protection mechanisms will be utilized to safeguard Association-Provided Information Systems and Equipment. Regular updates to the scanning software will be automatically pushed to Association-Provided Information Systems and Equipment to ensure detection of new threats. Employees, Directors, Agents, and Third Party Service Providers will not disable or circumvent threat prevention mechanisms.

Incident Response

The Association's Incident Response Program will promptly assess and manage security events to minimize their impact on the Association's operations, assets, and reputation. By establishing clear roles, responsibilities, and procedures, the Incident Response Program will enhance the Association's resilience against security threats, restore normal operations efficiently, and gain insights to enhance future incident handling capabilities and practices.

- An Incident Response Plan will be reviewed, updated, and approved annually by the Executive Leadership Team (ELT).
- The Incident Response Plan will contain procedures for assessing the nature and scope of an incident, containment, resolution, notifications, preservation of forensic evidence, and business resumption of business operations.
- Association leadership will report within twelve (12) hours any significant or critical security incidents affecting the ongoing operations or reputation of the Association to the Association Board and will report to the FCA and any local, state or federal authorities as appropriate.

Security Awareness

The Association will promote a culture of vigilance and preparedness by educating Employees and Directors about security risks and best practices. Through regular training and testing initiatives, the Association will enhance its resilience against cyber threats, ensuring that the Association remains informed and capable of identifying, mitigating, and responding effectively.

- All Employees and Directors will participate in annual Security Awareness training.
- Third Party Service Providers with access to confidential or sensitive information and/or Association-Provided Information Systems and Equipment will be contractually required to participate in Security Awareness training on a regular basis through the service provider.
- The Security Awareness training will encompass a range of subjects reflecting present threats and industry standards to identify opportunities for new behaviors and actions while reinforcing ongoing habits and routines.
- Employees with elevated permissions will participate in supplementary development focused on understanding, developing, and implementing appropriate security standards.

Internet Usage and Remote Access

The Association will establish appropriate standards for safe and secure utilization of internet resources and remote connectivity within the Association. Through acceptable practices, security measures, and industry best practices, the Association will mature capabilities to mitigate risks associated with unauthorized access, data compromise, and cyber threats while facilitating efficient and secure remote operations. Additionally, the

Association will continue to develop new capabilities to safeguard confidential or sensitive information, uphold regulatory compliance, and promote responsible use of Association resources, thereby maintaining the integrity and security of the Association's network infrastructure and digital assets.

- The Association will grant Internet connectivity unless the content is explicitly prohibited or restricted by the content filtering measures in place.
- Association Employees, Directors, Agents, and Third Party Service Providers utilizing Association-Provided Information Systems and Equipment to access the Internet will refrain from prohibited activities such as:
    - Accessing or distributing unauthorized or illegal materials.
    - Engaging in activities that could compromise the security of Association systems or networks.
    - Visiting websites known for hosting malicious content or engaging in phishing attempts.
    - Using internet resources for personal gain or non-work-related activities.
- All internet web services, sites, and digital publications bearing the Association's branding must undergo approval and publication by designated Association personnel to guarantee the disclosure of requisite notices and maintain a uniform public image.
- Remote access by Employees, Directors, Agents, and Third Party Service Providers to Association-Provided Information Systems and Equipment via the internet will be allowed with appropriate security and monitoring controls.
- Transmission of confidential or sensitive Association, Customer, Applicant, Director or Employee data across the internet will be prohibited unless it has been secured by an approved method of encryption. The sharing of Association, Customer, Applicant, Director, Employee, or other confidential or sensitive data via the internet must be done in compliance with Policy F.400: Disclosure and Release of Information and Policy OP.301: Enterprise Content Management.

Personal Email

The Association will establish standards for the appropriate and secure use of personal email accounts within the Association with clear expectations, limitations, and restrictions.

- Using personal email to send confidential or sensitive Association, Customer, Applicant, Director or Employee information poses significant risk to the security and confidentiality of the information. Employees, Directors, Agents, and Third Party Service Providers will not utilize personal email in any official capacity to transmit confidential or sensitive Association, Customer, Applicant, Director or Employee information.
- The Association will utilize suitable technology solutions to filter personal email communications for any instances of confidential or

sensitive information being transmitted from Association-Provided Information Systems and Equipment.
- The Association will utilize suitable technology solutions to detect and prevent cyber threats linked with personal email, including malicious links and attachments.

Delegated Authorities

Association leadership is hereby delegated authority to:

- develop and implement standards (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.

Reporting Requirements

To the greatest extent possible, policy reporting will 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 security practices and capabilities;
- Quarterly progress reports concerning the Association's Security Plan activities;
- Quarterly updates on key performance and risk metrics; and
- Quarterly updates on current and emerging security risks

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.