

**ASSOCIATED BANC-CORP  
ASSOCIATED BANK, NATIONAL ASSOCIATION  
ASSOCIATED TRUST COMPANY, NATIONAL ASSOCIATION**

**BOARD OF DIRECTORS**

**TECHNOLOGY COMMITTEE CHARTER**

**Purpose**

The purpose of the Technology Committee (the “Committee”) is to provide oversight and to promote effective governance related to the information technology strategy and technology-related operations and risk management of Associated Banc-Corp and its subsidiaries (collectively, the “Company”), including oversight of significant information technology investments in areas such as cybersecurity, strategy, risk management and emerging technology developments. The Committee shall assist the Board of Directors (the “Board”) and its other committees that oversee specific risk-related issues and serve as a resource to management.

**Committee Membership**

The Committee shall consist of no fewer than three members, the majority of whom shall be “independent” directors as defined by applicable law, including the rules and regulations of the Securities and Exchange Commission and the rules of The New York Stock Exchange.

**Meetings**

The Committee shall meet as often as it determines necessary, but not less frequently than quarterly. The Committee shall also meet separately with the Chief Information Officer, the Chief Information Security Officer, the Chief Risk Officer, and the General Counsel as often as it determines necessary. The Committee may request any officer or employee of the Company or any other person to attend a meeting of the Committee or to meet with any members of the Committee. For a portion or all of each of its meetings, the Committee may meet in executive session without any employees of the Company present.

The Committee may conduct its business and affairs at any time or location it deems appropriate. Attendance and participation in a meeting may take place by conference telephone or similar communications equipment by means of which all persons participating in the meeting can hear each other. Any action to be taken at any meeting of the Committee may be taken without a meeting, if all members of the Committee consent thereto in writing and such writing or writings are filed with the minutes of the Committee. All decisions of the Committee shall be determined by an affirmative vote of the majority of members in attendance. A quorum of the Committee shall be established when a majority of the members of the Committee are present.

**Authority and Responsibilities**

The Committee has the following responsibilities and duties, as well as responsibilities and duties with respect to any additional matters which may be referred to the Committee from time to time by the Board or the Chairman of the Board or which the Committee raises on its own initiative

(including the ability to designate and delegate duties to such standing and ad-hoc committees as it deems necessary):

1. Review and approve the development and implementation of the Company's data management, information technology, information security and third party management programs, policies, controls, strategies, and of measures taken by the Company to identify, assess, monitor, control and mitigate its risks in such areas, including (without limitation) review and approval of the following policies:
  - Data Governance Policy
  - Information Security Policy
  - Information Technology Policy
  - Third Party Management Policy
2. Through the Committee or the Committee Chair in consultation with members of the Committee as appropriate, meet jointly or communicate with the Enterprise Risk Committee of the Board or its Chair to review and discuss as necessary or appropriate cybersecurity, information security, and other technology risks to the Company.
3. Assess the likelihood, frequency and severity of cyber-attacks and data breaches and review management's action plan for and response during any significant cyber-attack or data breach, which may include management's investigation of the incident, law enforcement engagement, customer, media and/or regulatory notification and disclosure, reporting and remediation.
4. Review the scope and effectiveness of the Company's material information technology and information security infrastructure, including strategies for the design, development, implementation and maintenance of new technologies and systems.
5. Review and discuss with management reports on the Company's technology strategy and operations, significant technology investments and related technological progress, and trends that may affect the Company's technology strategy and operations.
6. Review and discuss with management reports on the Company's strategies for capitalizing on industry changes and new distribution channels for products and services created by digital technologies.
7. Review and oversee significant Company investments in technology, technological infrastructure, and cybersecurity, and assess related program needs.
8. Review and monitor material vendor relationships related to information technology, including (without limitation) information technology outsourcing relationships.
9. Make regular reports to the Board summarizing the actions taken at each Committee meeting.
10. Annually review its own performance and assess the adequacy of this Charter. The Committee may recommend amendments to this Charter at any time and submit amendments for approval to the Board.

## **Retention of Consultants and Advisors**

The Committee shall have the authority to hire and terminate any consulting, legal or other advisors, such as cybersecurity consultants or breach counsel, as it deems appropriate to properly discharge its authority and responsibilities, including sole authority to approve such consultants' or advisors' fees and other retention terms, and shall be directly responsible for the oversight of their work. The Company shall provide appropriate funding, as determined by the Committee, for payment of reasonable compensation to any consultants or advisors retained by the Committee.

## **Limitation of the Committee's Role**

In exercising its oversight role, the Committee is entitled to rely on management to assume the primary responsibility for the effectiveness of the Company's information technology risk program, including the responsibility to establish appropriate policies, practices, and procedures. The Committee will also be entitled to rely on the periodic reports from management in addressing these programs, policies, practices and procedures.

37263104.2