

**EQUIFAX INC.**  
**CHARTER OF THE TECHNOLOGY COMMITTEE**  
**OF THE BOARD OF DIRECTORS**

**I. PURPOSE**

The purpose of the Technology Committee (the “Committee”) is to assist the Board of Directors (the “Board”) of Equifax Inc. (the “Company”) with respect to its oversight of (i) the Company’s technology strategy and significant technology investments in support of its evolving global business needs and (ii) cybersecurity and technology-related risks and management efforts to monitor and mitigate those risks. Areas of review include: information technology strategy; significant new product lines or technology investments; and the Company’s response to technology-based threats and opportunities. In addition, the Committee will oversee the Company’s mitigation of any identified enterprise-wide risks in the above areas.

**II. MEMBERS**

The Committee shall consist of three or more directors as determined and appointed by the Board. Each of these directors shall be independent in accordance with New York Stock Exchange rules. The following skills are particularly useful for the Committee members to have: familiarity and experience with technology development and/or deployment; technology strategy; and technology risk assessment and management, including data security risk management.

**III. MEETINGS**

1. The Committee shall meet at least quarterly and at such other times as determined by the Chair of the Committee or a majority of the Committee members.
2. The Board may appoint a Chair of the Committee. The Chair will preside, when present, at all meetings of the Committee. A majority of the members of the Committee shall constitute a quorum for the transaction of business. A majority of the members present at any meeting at which a quorum is present may act on behalf of the Committee. The Committee may meet by audio or videoconference and may take action by written consent.
3. To foster open and candid communication, the Committee will meet with management and outside advisors performing reviews of the Company’s cybersecurity program in separate executive sessions.
4. The Committee will report its activities and findings to the Board on a regular basis.

#### **IV. RESPONSIBILITIES AND DUTIES**

The specific duties and responsibilities of the Committee are set forth below. Unless otherwise specified, the intervals for review of any given policy or program may be annual, biannual, or at longer or shorter intervals, depending upon the nature of the subject matter and developments affecting the Company with respect to that subject matter.

##### **A. Technology Strategy and Investments**

1. Review the information technology strategy of the Company in light of the Company's evolving global business needs.
2. Review and report to the Board with respect to the resources allocated to technology.
3. Monitor significant new technology product development programs (including software initiatives) and new technology investments, including technical and market risks associated with product development and investment.
4. Monitor and oversee Company review of future trends in technology that may affect the Company's strategic plans, including overall industry trends and new opportunities and threats occasioned by new technologies, especially disruptive technologies.
5. Assess the scope and quality of the Company's intellectual property portfolio and strategy.

##### **B. Cybersecurity and Technology-Related Risk Management**

1. In coordination with the Audit Committee, oversee risk management with respect to cybersecurity. The Committee may, as it deems appropriate, hold joint meetings of the Audit Committee and the Committee regarding risk management with respect to cybersecurity or other appropriate matters.
2. Review with management the Company's technology investments and infrastructure associated with risk management, including policies relating to information security, disaster recovery and business continuity.
3. Review with management the effectiveness of the Company's cybersecurity program and all major changes and improvements pertaining to the Company's cybersecurity controls and plans.
4. Receive reports on the Company's technical security architecture.
5. Review and report to the Board with respect to the resources allocated to cybersecurity.

6. Review with management and report to the Board with respect to the root cause and remediation efforts with respect to all material cybersecurity incidents.
7. Review with management and report to the Board with respect to technology aspects of business continuity planning.
8. Review with management the effectiveness of the Company's escalation protocols with respect to prompt reporting of cybersecurity incidents to management, the Committee and the Board.
9. In coordination with the Audit Committee, review periodic internal reports to management with respect to information technology and cybersecurity issues prepared by the internal audit department and management's response along with the status of prior outstanding recommendations.

C. Outside Cybersecurity Advisors

1. Oversee the selection, appointment and retention (by the Committee or otherwise) of outside advisors to review the Company's cybersecurity program and to otherwise support the work of the Committee.
2. Review the plans and methodology for the periodic review and assessment of the Company's cybersecurity program by outside advisors.
3. Review with management the findings of reviews of the Company's cybersecurity program by outside advisors and remediation plans to address any material control deficiencies identified.

D. Other

1. Meet as appropriate, and at least annually, with the Company's Chief Information Security Officer and Chief Technology Officer in executive session to discuss information technology and cybersecurity risks, programs, activities, opportunities and developments.
2. Undertake from time to time such additional activities within the scope of the Committee's primary purposes as it may deem appropriate and/or as assigned by the Board of Directors.

**V. GENERAL PROVISIONS**

1. The Committee may establish such subcommittees of its members as it deems appropriate to assist it in its duties.
2. In the course of fulfilling its duties, the Committee may at any time seek advice and assistance from outside technology or cybersecurity consultants or other advisors, including outside legal counsel, as the Committee deems necessary or

appropriate to carry out its duties on such terms as the Committee, in its sole discretion, shall determine to be fair and reasonable without necessity for Board approval.

3. The Committee shall receive appropriate funding, as it determines, from the Company for payment of compensation to any outside technology or cybersecurity consultants, other advisors or outside legal counsel engaged by the Committee, and for ordinary administrative expenses of the Committee that are necessary or appropriate in carrying out its duties.
4. The Committee shall conduct an annual performance self-evaluation and report the results of such evaluation to the Governance Committee.
5. The Committee shall review and assess the adequacy of this Charter at least annually and report the results of such review to the Governance Committee.

\* \* \* \* \*

Last revised February 7, 2024