

FedEx Corporation

Cyber and Technology Oversight Committee Charter

Purpose

The purpose of the Cyber and Technology Oversight Committee is to:

- Review major cyber and technology-related projects and technology architecture decisions;
- Assess whether the Company's cyber and technology programs effectively support the Company's business objectives and strategies;
- Assist Board oversight of cyber and technology-related risks and management efforts to monitor and mitigate those risks;
- Advise the Company's senior Information Technology ("IT") management team; and
- Advise the Board of Directors on cyber and technology-related matters.

Membership and Subcommittees

The Cyber and Technology Oversight Committee shall consist of such number of members of the Board of Directors as shall be appointed by the Board from time to time, but in no event shall the Committee consist of fewer than three members. The Board of Directors shall designate the Chairperson of the Committee. The Board of Directors may change the membership of the Committee at any time.

Unless otherwise prohibited by the Company's Certificate of Incorporation or Bylaws, the Committee may form and delegate authority to any subcommittee as it deems appropriate or advisable.

Functions, Powers, and Responsibilities

The Cyber and Technology Oversight Committee shall:

Cyber and Technology Projects

1. Review and discuss with management the financial, tactical, and strategic benefits of proposed major cyber and technology-related projects and technology architecture alternatives.
2. Review and discuss with management the progress of major cyber and technology-related projects and technology architecture decisions.
3. Make recommendations to the Board of Directors with respect to cyber and technology-related projects and investments that require Board approval.

Cyber and Technology Risk Management

4. Review and discuss with management and the Board of Directors (i) the Company's cyber and technology-related risks, including network security, information security, and data privacy and protection, and (ii) the steps management has taken to identify, assess, monitor, manage, and mitigate those risks.

5. Review and discuss with management (i) technologies, policies, processes, and practices for managing and mitigating cyber and technology-related risks and (ii) the Company's cyber incident response and recovery plan.

6. Review and discuss with management the cybersecurity, cyber-resiliency, and technology aspects of the Company's business continuity and disaster recovery capabilities and contingency plans.

Internal Controls

7. Review and discuss with management the quality and effectiveness of the technology systems and processes that relate to or affect the Company's internal control systems.

8. Review and discuss with management and the Board of Directors (i) the Company's cyber and technology-related compliance risks, including cyber and technology-related internal audits, and (ii) the steps management has taken to identify, assess, monitor, manage, and mitigate those risks.

9. Periodically report to and consult with the Audit Committee of the Board of Directors regarding cyber and technology systems and processes that relate to or affect the Company's internal control systems.

Advisory Role

10. Advise the Company's senior IT management team.

11. Stay informed of, assess, and advise the Company's senior IT management team with respect to trends, new technologies, applications, and systems that relate to or affect the Company's cyber and technology strategy or programs.

Other

12. Annually review the Committee's own performance and report the results of such review to the Board of Directors.

13. Annually review and reassess the adequacy of this charter and recommend any proposed changes to the Board of Directors for approval.

14. Report regularly to the Board of Directors on matters within the scope of the Committee, as well as any special issues that merit the attention of the Board.

15. Perform such other duties as are necessary or appropriate to ensure that the Company's cyber and technology programs effectively support the Company's business objectives and strategies, or as the Board of Directors may from time to time direct.

Amended March 7, 2022