

CITRIX SYSTEMS, INC.

Technology, Data and Information Security Committee Charter

A. PURPOSE AND SCOPE

The primary function of the Technology, Data and Information Security Committee (the “Committee”) of the Board of Directors (the “Board”) of Citrix Systems, Inc. (the “Corporation”) is to exercise the responsibilities and duties set forth below, including, but not limited to, oversight of the Corporation’s information technology use and protection, including review and oversight of the Corporation’s policies, plans and programs relating to enterprise cybersecurity and data protection risks associated with the Corporation’s products, services, information technology infrastructure and related operations.

B. COMPOSITION

The Committee shall be comprised of a minimum of three members of the Board as appointed by the Board.

The Board shall appoint the members of the Committee annually. Each member of the Committee shall serve until his or her successor shall be duly appointed and qualified or until his or her earlier resignation or removal. Unless a Chair is elected by the full Board, the members of the Committee may designate a Chair by majority vote of the full Committee membership.

The Committee shall meet as necessary, but at least four times each year, to enable it to fulfill its responsibilities and duties as set forth herein. The Committee may invite members of management or others to attend Committee meetings and provide pertinent information as the Committee may request on the issues being considered.

The Committee shall report its actions to the Board and keep written minutes of its meetings, which shall be recorded and filed with the books and records of the Corporation.

C. RESPONSIBILITIES AND DUTIES

To fulfill its responsibilities and duties the Committee shall:

1. *Enterprise Cybersecurity* – Oversee and assess the quality and effectiveness of the Corporation’s cybersecurity team, technology, policies and procedures protecting the Corporation’s information technology systems, data, products and services across all business functions.
2. *Incident Monitoring and Response* –
 - Oversee and review periodically the Corporation’s controls to prevent, detect and respond to cyber-attacks or data breaches involving the Corporation’s information technology systems, data, products and services, taking into account the potential for external and internal threats to the Corporation and its customers, partners, vendors and employees.

- Review and approve on a periodic basis (but at least annually) the Corporation's incident response plans, policies and frameworks, including policies for the escalation and reporting of significant security incidents to the Board, regulatory agencies and law enforcement, as appropriate.
3. *Data Privacy and Security* – Oversee the Corporation's compliance with global data privacy and security regulations and requirements applicable to the data the Corporation receives, collects, creates, uses, processes and maintains (including personal information and information regarding customers, partners and vendors) and assess the effectiveness of the systems, controls and procedures used by the Corporation to ensure compliance with applicable global data privacy and security regulations and requirements.
 4. *Business Continuity Planning and Disaster Recovery* –
 - Review periodically with management the Corporation's business continuity and disaster recovery capabilities.
 - Review and approve on a periodic basis (but at least annually) the Corporation's business continuity and disaster recovery plans, policies and frameworks.
 5. *Compliance Risks and Audits* – In coordination with the Corporation's Audit Committee, oversee the Corporation's management of risks related to its information technology systems and processes, including privacy, network security and data security, and any audits of such systems and processes.
 6. *Product and Information Technology Strategies and Operational Plans* – Review the Corporation's strategies and operational plans relating to the development, deployment, integration and servicing of products, services, applications and systems (including policies, procedures and controls related thereto) to identify and mitigate data security and privacy risks in such strategies and programs.
 7. *IT and Security Funding* – Oversee the Corporation's funding and resourcing of its information technology and security functions.
 8. *Insurance* – In coordination with the Corporation's Audit Committee, annually review the appropriateness and adequacy of the Corporation's technology and cyber risk insurance coverage.
 9. *Technology Landscape and Trends* – Monitor and discuss, with the Corporation's management, emerging security, data protection and privacy trends in the technology landscape.
 10. *General Authority* – Exercise such additional powers and duties as may be reasonable, necessary or desirable, in the Committee's discretion, to fulfill its duties under this Charter.

D. INDEPENDENT ADVICE

The Committee may conduct or authorize audits, investigations into or studies of matters within the Committee's scope of responsibilities and duties, as described above. In carrying out its duties and responsibilities, the Committee shall have the authority to appoint, retain, compensate, terminate and oversee the work of any independent experts, consultants, legal counsel and other advisers and instruct such experts, consultants, legal counsel and advisers that they should report directly to the Committee on matters pertaining to the work performed during their engagement.

The Committee shall exercise sole authority to approve any reasonable fees and other retention terms of any expert, consultant, legal counsel or other adviser that is to be used by the Committee, such funding to be provided by the Corporation.

E. CHARTER AND EVALUATIONS

The Committee shall periodically, but at least annually, review and assess the adequacy of this Charter and recommend any modifications to this Charter, if and when appropriate, to the Board for its approval. The Committee shall periodically evaluate its own performance and report the results of such evaluation to the Board.

Adopted by the Board of Directors: September 17, 2019