Approved June 3, 2015

Tech Data Corporation
Cybersecurity Committee Charter

I. Scope	The Cybersecurity Committee (the "Committee") is a committee of the Board of Directors (the "Board") established pursuant to the Bylaws of Tech Data Corporation (the "Corporation"). The Committee assists the Board in: • Setting expectations and accountability of management regarding cybersecurity preparedness • Assessing the adequacy of resources and funding to sustain a successful cybersecurity program • Providing advice and recommendations related to enhancing existing and developing future cybersecurity and data privacy initiatives
II. Composition	The members of the Committee will be elected as described in the Bylaws. The Committee will be comprised of two or more directors. All members must be independent.
III. Meetings	The Committee will meet at least once per year and as often as necessary to carry out its responsibilities. All meetings will be held pursuant to the Bylaws and written minutes of each meeting must be duly filed in the Corporation records. Reports of meetings of the Committee will be made to the Board at its next regularly scheduled meeting following the Committee meeting.
IV. Responsibilities and Duties	The Committee's primary duties and responsibilities are to: 1. Review the Company's overall cybersecurity plan and information technology information protection management strategy related risks. The committee shall be provided the results of any audit of the Company's cybersecurity plan and shall receive regular updates on cybersecurity and data protection and privacy. 2. Review reports from the Legal Department regarding legal implications of cyber risks posed to the Company, including those related to potential data breaches and to maintain awareness of regulatory issues, monitor adherence to legal requirements; and monitor disclosure and reporting activities. 3. Review reports provided by the Information Technology organization regarding the status of and future plans for the security of Company data stored on internal resources and with third party providers. 4. Review and make recommendations related to strategy, as appropriate, regarding action plans related to responses to data breaches. 5. Have the authority and funding from the Corporation to obtain advice and seek assistance from outside cybersecurity and data privacy advisors and consultants as it determines necessary to carry out its duties. 6. Review and advise on resources and funding issues relating to the establishment and maintenance of adequate cybersecurity controls and processes and information management protection risks.