DYNATRACE, INC.

CYBERSECURITY COMMITTEE CHARTER

I. General Statement of Purpose

The purposes of the Cybersecurity Committee (the "**Cybersecurity Committee**") of the Board of Directors (the "**Board**") of Dynatrace, Inc. (the "**Company**") are to:

- manage oversight of the Company's investments, programs, plans, controls, and policies relating to cybersecurity, data privacy and data protection risks associated with its products, services, and business operations;

- provide feedback on cybersecurity-related matters, including, but not limited to, strategies, objectives, capabilities, initiatives, and policies; and

- oversee other tasks related to the Company's cybersecurity and data privacy functions as the Board may delegate to the Cybersecurity Committee from time to time.

The Cybersecurity Committee will primarily fulfill these responsibilities by carrying out the activities enumerated in Section IV of this Charter.

II. Composition

The Cybersecurity Committee shall be comprised of one or more directors, all of whom are members of the Board, which shall also fix the size of the Cybersecurity Committee. The members of the Cybersecurity Committee will be appointed by the Board and will serve at the pleasure of the Board. Any vacancy on the Cybersecurity Committee will be filled by, and any member of the Cybersecurity Committee may be removed as such by, an affirmative vote of the majority of the Board. Subject to the provisions of the Company's certificate of incorporation and/or the Company's bylaws, unless the Board designates a chairperson of the Cybersecurity Committee, the members of the Cybersecurity Committee may designate a chairperson and change that designation by an affirmative vote of the majority of the full Cybersecurity Committee membership. The chairperson shall be responsible for leadership of the Cybersecurity Committee, including presiding over the meetings of the Cybersecurity Committee and reporting to the Board. Subject to the provisions of the Company's certificate of incorporation and/or the Company's bylaws, the Board may remove or replace the chairperson of the Cybersecurity Committee at any time by an affirmative vote of the majority of the Board. Notwithstanding the foregoing membership requirements and subject to applicable law, no action of the Cybersecurity Committee will be invalid by reason of any such requirement not being met at the time the action is taken.

III. Meetings

The Cybersecurity Committee will meet as often as it deems appropriate to carry out its responsibilities under this charter (the "**Charter**"), but not less frequently than quarterly.

At every meeting of the Cybersecurity Committee, the presence of a majority of all the members shall constitute a quorum, and the affirmative vote of a majority of members present shall be necessary for the adoption by it of any resolution. The Cybersecurity Committee may also act by unanimous written consent (which may include electronic consent) in lieu of a meeting to the extent permitted by the Company's bylaws, as may be adopted and amended by the Board from time to time.

Meetings may, at the discretion of the Cybersecurity Committee, include other directors, members of the Company's management, independent consultants or advisors, or such other persons as the Cybersecurity Committee or its chairperson may determine. Those in attendance who are not members of the Cybersecurity Committee may observe, but may not participate in, any discussion or deliberation unless invited to do so by the Cybersecurity Committee, and in any event, are not entitled to vote at the meeting. The Cybersecurity Committee may also exclude from its meetings (or portions thereof) any person it deems appropriate, other than members of the Cybersecurity Committee.

The Company's Chief Technology Officer, key members of the Company's Information Security Office, the General Counsel and such other officer(s) and members of senior management as may be appropriate shall act as management liaisons to the Cybersecurity Committee and shall work with the Cybersecurity Committee chairperson to prepare an agenda for regularly scheduled meetings. The Cybersecurity Committee chairperson will make the final decision regarding the agenda for regularly scheduled meetings and shall develop the agenda for special meetings based on the information supplied by the persons requesting the special meeting.

The agenda and all materials to be reviewed at the meetings should be received by the Cybersecurity Committee members as far in advance of the meeting day as practicable.

The Cybersecurity Committee shall make regular reports to the Board about its activities and decisions, which may be made through the chairperson.

Except as expressly provided in this Charter, the Company's certificate of incorporation, the Company's bylaws, or the Corporate Governance Guidelines of the Company, the Cybersecurity Committee may determine additional rules and procedures to govern it or any of its subcommittees, including designation of a chairperson *pro tempore* in the absence of the chairperson and designation of a secretary of the Cybersecurity Committee or any meeting thereof.

IV. Authority and Delegation and Responsibilities

The Cybersecurity Committee is delegated all authority of the Board as may be required or advisable to fulfill the purposes of the Cybersecurity Committee. The Cybersecurity Committee may form and delegate some or all of its authority to subcommittees when it deems appropriate.

The Cybersecurity Committee shall review and reassess the adequacy of this Charter annually and recommend to the Board any amendments or modifications to the Charter that the Cybersecurity Committee deems appropriate.

At least annually, the Cybersecurity Committee shall evaluate its own performance and report the results of such evaluation to the Board and the Nominating and Corporate Governance Committee.

The Cybersecurity Committee shall have the authority to retain and terminate outside counsel, advisors or other experts or consultants, as it deems appropriate, including complete authority to approve their fees and other retention terms. The Company must provide for appropriate funding, as determined by the Cybersecurity Committee, for payment of reasonable compensation to outside counsel, advisors, or other experts or consultants retained by the Cybersecurity Committee. Any communications between the Cybersecurity Committee and legal counsel while obtaining legal advice will be privileged communications of the Company and the Cybersecurity Committee will take all necessary steps to preserve the privileged nature of those communications. The Cybersecurity Committee may require any officer or employee of the Company or any of its subsidiaries or the Company's outside legal counsel and any outside consultants or advisors to the Company

to attend a meeting of the Cybersecurity Committee or to meet with any member of or advisor or consultant to the Cybersecurity Committee.

Without limiting the generality of the foregoing statements but subject to the Corporate Governance Guidelines, the principal responsibilities of the Cybersecurity Committee are to review, advise and take action as necessary on the following matters:

1. The effectiveness of the Company's cybersecurity programs and its practices for identifying, assessing, and mitigating cybersecurity risks across the Company's products, services, and business operations;

2. The Company's controls, policies and guidelines to prevent, detect, and respond to cyber incidents or data breaches involving the Company's products, services, data, information systems, and business operations;

3. The Company's security strategy and technology planning processes;

4. The safeguards used to protect the confidentiality, integrity, availability and resiliency of the Company's products, services, and business operations;

5. The Company's cyber crisis preparedness, security breach and incident response plans, communication plans, and disaster recovery and business continuity capabilities;

6. The Company's compliance with applicable information security, data privacy and data protection laws and industry standards;

7. The Company's cybersecurity budget, investments, training, and staffing levels to ensure they are sufficient to sustain and advance successful cybersecurity and industry compliance programs;

8. The threat landscape facing the Company and the Company's products, services, and business operations;

9. Any new or updated legal implications of security, data privacy, and/or other regulatory or compliance risks to the Company or the Company's products, services, and business operations; and

10. Other matters as the Cybersecurity Committee chairperson or other members of the Cybersecurity Committee determine relevant to the Cybersecurity Committee's oversight of cybersecurity programs and risk assessment and management.

*****

As amended on July 11, 2023.