CHARTER
OF THE
CYBERSECURITY AND DATA PROTECTION COMMITTEE
OF THE
BOARD OF DIRECTORS
OF
BROADSOFT, INC.

PURPOSE

The purpose of the Cybersecurity and Data Protection Committee (the "Committee") of the Board of Directors (the "Board") of BroadSoft, Inc. (the "Company") shall be to act on behalf of the Board in fulfilling the Board's responsibilities to oversee the Company's policies, plans and programs relating to cybersecurity and data protection risks.

COMPOSITION

The Committee shall consist of at least two (2) members of the Board. The members of the Committee shall be appointed by and serve at the discretion of the Board. Vacancies occurring on the Committee shall be filled by the Board and the Committee's chairperson shall be designated by the Board.

MEETINGS, MINUTES AND REPORTS

The Committee shall hold such regular or special meetings as its members deem necessary, appropriate or desirable, but in no event less than annually. The presence in person or by telephone of a majority of the Committee's members shall constitute a quorum for any meeting of the Committee.

Minutes of each meeting of the Committee shall be prepared and distributed to each member of the Committee, members of the Board who are not members of the Committee, and the Secretary of the Company, and shall be placed in the Company's minute book. The Chair of the Committee shall report to the Board from time to time and whenever requested by the Board.

AUTHORITY

The Committee shall have full access to all books, records, facilities and personnel of the Company as deemed necessary, appropriate or desirable by any member of the Committee to discharge his or her responsibilities hereunder, including access to the Company's Chief Information Officer ("CIO") and Chief Information Security Officer ("CISO"). The CIO and CISO shall be available to attend meetings of the Committee and shall update the Committee at the Committee's request, but at least quarterly on the status of the Company's cybersecurity and data protection strategy, plans and practices. The Committee may request that any directors, officers or other employees of the Company, or any other persons whose advice and counsel are sought by the Committee, attend any meeting of the Committee to provide such pertinent information as the

Committee requests. The Committee may exclude from its meetings any persons it deems appropriate in order for it to fulfill its responsibilities. The Committee shall have the authority to obtain, at the expense of the Company, advice and assistance from internal or external advisors and consultants.

RESPONSIBILITIES

The Committee shall have the following specific authority and responsibilities, in addition to any others that the Board may from time to time delegate to the Committee:

1. The Committee shall provide oversight with respect to the following Company cybersecurity and data protection matters:

    (a) the strength and effectiveness of the Company's cybersecurity and data protection processes, safeguards, resources and training;

    (b) the Company's information security and data protection planning processes;

    (c) the Company's focus on critical information security and protection technologies, their development and related innovations;

    (d) the security risks associated with the Company's information systems and operations;

    (e) the architecture, design and implementation of administrative, technical and physical safeguards intended to protect the confidentiality, integrity and availability of the Company's information and the resiliency of the Company's operations;

    (f) the Company's compliance with applicable information security and data protection laws, industry standards (e.g., ISO27001), processes (e.g., GRC), and frameworks (e.g., NIST); and

    (g) the threat landscape facing the Company and the Company's strategy and preparedness to identify and mitigate cybersecurity threats and vulnerabilities.

2. The Committee shall monitor the adoption of security processes within the Company to reduce the likelihood of security or data breaches.

3. The Committee shall meet with Company personnel and external advisors regarding cybersecurity and data protection matters, as the Committee deems necessary, appropriate or desirable.

4. The Committee shall regularly brief the Board with respect to cybersecurity and data protection risks, developments and issues.

5. The Committee will work closely with the Audit Committee of the Board to ensure related matters are addressed by the appropriate Board committee.

6. The Committee shall be notified promptly by the CIO or CISO of any material cybersecurity breach. All external reporting and public relations-related notifications shall also be shared promptly with the Committee. The CIO and CISO shall accept input, advice, and recommendations from the Committee regarding the handling of any serious cyber breaches that could have a significant impact on the Company's posture, reputation, and business.

Management is responsible for establishing and maintaining the integrity of the Company's cybersecurity and data protection internal controls, including identifying cybersecurity risks and vulnerabilities and implementing appropriate safeguards.