RAMBUS INC.
AI AND CYBER RISK COMMITTEE CHARTER
(As amended October 22, 2026)

I. PURPOSE

The purpose of the AI and Cyber Risk Committee (the "**Committee**") of the Board of Directors (the "**Board**") of Rambus Inc. (the "**Company**") shall be to assist the Board in fulfilling its oversight responsibilities with respect to the Company's information technology use, artificial intelligence systems and data security, including, but not limited to, enterprise cybersecurity, artificial intelligence governance, privacy, data collection and protection and compliance with information security, data protection, incident response and disaster recovery plans, and applicable artificial intelligence laws and regulations.

The Committee has the authority to undertake the specific duties and responsibilities as are enumerated in or consistent with this charter and will have the authority to undertake such other specific duties as the Board from time-to-time prescribes.

Without limiting the generality of the foregoing statements, but subject to the Company's Corporate Governance Guidelines, the charter and mission of the Committee are to review and advise on the following matters:

- The Company's security strategy and technology planning processes; including the Company's artificial intelligence strategy and governance framework;
- The effectiveness of the Company's cybersecurity and artificial intelligence programs and its practices for identifying, assessing, and mitigating cybersecurity and artificial intelligence risks across the Company's products, services, and business operations;
- 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;
- The threat landscape facing the Company and the Company's products, services, and business operations; and including emerging risks arising from artificial intelligence
- The safeguards used to protect the confidentiality, integrity, availability and resiliency of the Company's products, services, and business operations.

II. MEMBERSHIP

The Committee shall consist of at least two members of the Board. Members of the Committee shall be appointed by the Board upon the recommendation of the Corporate Governance and Nominating Committee and may be removed by the Board in its discretion. The members of the Committee shall meet such qualifications as may be established by the Board from time to time. The Board may designate a chairperson of the Committee. In the absence of that designation, the Committee may designate a chairperson by majority vote of the Committee members.

III. ROLES AND RESPONSIBILITIES

The Committee may perform such functions as are consistent with its purpose and applicable law, rules, and regulations and as the Board or the Committee deem appropriate. In carrying out its responsibilities, the Committee believes its policies and procedures should remain flexible, in order to best react to changing conditions and circumstances.

The following are the principal responsibilities of the Committee:

- ***Data Collection and Use.*** The Committee shall oversee the systems, controls and procedures used by the Company and business partners engaged by the Company to collect, create, use, maintain, process and protect personal information and/or any information or assets of the Company's customers, employees and business partners (collectively, "Company Information Assets"), including the use of Company Information Assets for training, fine-tuning or operating artificial intelligence systems.

- ***Data Protection.*** The Committee shall oversee policies, procedures, plans and execution intended to provide security, confidentiality, availability and integrity of Company Information Assets.

- ***Enterprise Cybersecurity***. The Committee shall oversee the quality and effectiveness of the Company's policies and procedures with respect to its information technology systems, including enterprise cybersecurity and privacy.

- ***Artificial Intelligence Oversight.*** The Committee shall oversee the Company's development, procurement and deployment of artificial intelligence systems, including review of governance frameworks, accountability measures, model risk assessments and safeguards designed to promote the responsible use of artificial intelligence across the Company's products, services and business operations.

- ***Incident Response.*** The Committee shall review and provide oversight on the policies and procedures of the Company in preparation for responding to any artificial intelligence or data security incidents. Review with management the root cause of and remediation efforts with respect to all material cybersecurity incidents.

- ***Disaster Recovery.*** The Committee shall review periodically with management the Company's disaster recovery, business continuity, and business resiliency capabilities.

- ***Compliance Security Risks and Audits.*** The Committee shall oversee the Company's management of internal and external risks related to its information technology and artificial intelligence systems and processes, including encryption, network security, data security, artificial intelligence model integrity, risk management frameworks, compliance with applicable artificial intelligence and cybersecurity regulations, and any internal or third-party audits of such systems and processes.

- ***Access Controls.*** The Committee shall review with management the quality and effectiveness of IT systems and processes that relate to the Company's internal access control systems, including physical, organizational, and technical security.

- ***Cyber Insurance.*** The Committee may review the Company's cyber insurance policies to ensure appropriate coverage.

- ***Retention of Consultants and Advisors; Investigations***. The Committee may undertake the following activities and responsibilities with respect to retaining consultants or advisors and authorizing investigations (in addition to any others that the Board may from time-to-time delegate to the Committee):

    - The Committee shall have the authority, without having to seek Board approval, to obtain, at the expense of the Company, advice and assistance from cybersecurity, artificial intelligence or data privacy experts or consultants or other advisors as it deems advisable.

    - The Committee shall have the authority to conduct or authorize investigations into or studies of any matters within the Committee's scope of responsibilities.

IV. ORGANIZATIONAL MATTERS

Meetings: The Committee will hold meetings as often as may be deemed necessary or appropriate, in its judgment, in order to fulfill its responsibilities, but in any event at least quarterly. The Committee will keep regular minutes of its meetings and will regularly update the Board about Committee activities and findings.

Authority to Mandate Attendance: 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.

Review of Committee Performance and Charter: The Committee may review its own performance and reassess the adequacy of this charter in such manner as it deems appropriate, and submit such evaluation, including any recommendations for change coming from the Committee or counsel, to the full Board for review, discussion and approval, at least annually.

Committee Rules: Unless the Board, the Company's Bylaws or this charter provides otherwise, the Committee may make, alter or repeal rules for the conduct of its affairs. All references to specific statutes or regulations in this charter are to such statutes or regulations as they may be amended from time to time in the future.