

POWER INTEGRATIONS, INC.
CHARTER OF THE CYBERSECURITY COMMITTEE
OF THE BOARD OF DIRECTORS

(Adopted October 28, 2025)

I. PURPOSE

This Charter specifies the scope of the responsibilities of the Cybersecurity Committee (the “Committee”) of the Board of Directors (the “Board”) of Power Integrations, Inc. (the “Company”) and the manner in which those responsibilities shall be performed, including its structure, processes and membership requirements.

The primary purpose of the Committee is to assist the Board in fulfilling its oversight responsibilities with respect to the Company’s information technology use and data security, including, but not limited to, enterprise cybersecurity, privacy, data collection and protection and compliance with information security and data protection laws.

In carrying out these responsibilities, the Committee shall review and advise on: (i) the Company’s security strategy and technology planning processes; (ii) the effectiveness of the Company’s cybersecurity programs and its practices for identifying, assessing, and mitigating cybersecurity risks across the Company’s business operations; (iii) the Company’s cybersecurity budget, investments, training, and staffing levels to ensure they are sufficient to sustain and advance cybersecurity and industry compliance programs; (iv) the threat landscape facing the Company and the Company’s business operations; and (v) the safeguards used to protect the confidentiality, integrity, availability and resiliency of the Company’s business operations.

II. ORGANIZATION AND MEMBERSHIP REQUIREMENTS

The Committee shall consist of at least two directors. The members of the Committee shall be appointed by the Board on the recommendation of the Nominating and Governance Committee and shall serve until their successors are duly elected and qualified or their earlier resignation or removal. Any member of the Committee may be removed or replaced by the Board. The members of the Committee shall meet such qualifications as may be established by the Board from time to time, and at least one of such members shall have relevant experience in cybersecurity/IT related risks and if no director is available for service on the Committee with such experience, the Committee shall retain cybersecurity or data privacy experts or consultants or other advisors that have such experience. The Committee may from time to time delegate duties or responsibilities to subcommittees or to one member of the Committee. The Board shall designate the chair of the Committee.

III. MEETINGS

The Committee shall meet as often as it deems necessary to fulfill its responsibilities hereunder, but not less frequently than quarterly each year, and may meet with management or

individual directors at any time it deems appropriate to discuss any matters before the Committee.

The Committee shall maintain written minutes of its meetings, which minutes will be filed with the minutes of the meetings of the Board.

The Committee will present its recommendations to the Board in form and substance as determined by the Committee or as otherwise directed by the Board, and shall provide not less frequently than annually updates to the Board on cybersecurity trends, threats and regulatory developments.

IV. COMMITTEE AUTHORITY AND RESPONSIBILITIES

To implement the Committee's purpose and policies, the Committee shall be charged with the following duties and responsibilities. The Committee may supplement and, except as otherwise required by applicable law or the requirements of Nasdaq, deviate from these activities as appropriate under the circumstances:

- A. Data Collection.** The Committee shall review and provide oversight of 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").
- B. Data Protection.** The Committee shall review and provide oversight of policies, procedures, plans and execution intended to provide security, confidentiality, availability and integrity of Company Information Assets.
- C. Enterprise Cybersecurity.** The Committee shall review and provide oversight of the quality and effectiveness of the Company's policies and procedures with respect to its information technology systems, including enterprise cybersecurity and privacy.
- D. Incident Response.** The Committee shall review and provide oversight on the policies and procedures of the Company in preparation for responding to any data security incidents. Review with management the root cause of and remediation efforts with respect to all material cybersecurity incidents.
- E. Disaster Recovery.** The Committee shall review periodically with management the Company's disaster recovery, business continuity, and business resiliency capabilities.
- F. Compliance Security Risks and Audits.** The Committee shall oversee the Company's management of internal and external risks related to its information technology systems and processes, including encryption, network security, data security, risk management frameworks, and any internal or third-party audits of such systems and processes, and shall review with the Company's management such risks as they may be affected by the Company's expansion into new product lines, new geographies, or mergers and acquisitions among other things.

- G. 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.
- H. Cyber Insurance.** The Committee shall annually review the Company's cyber insurance policies to ensure appropriate coverage.
- I. Cybersecurity Disclosure Requirements.** The Committee shall oversee and review with management the Company's cybersecurity-related disclosure controls and procedures and alignment with applicable regulations.
- J. Cybersecurity Budget Review.** The Committee shall review with management the Company's cybersecurity-related budgetary items.
- K.** Review and reassess this Charter's adequacy as appropriate, but no less than once per year.
- L. 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):
1. 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 or data privacy experts or consultants or other advisors as it deems advisable.
 2. The Committee shall have the authority to conduct or authorize investigations into or studies of any matters within the Committee's scope of responsibilities.