

CYBERSECURITY RISK MANAGEMENT COMMITTEE CHARTER

PURPOSE

The Cybersecurity Risk Management Committee (the “Committee”) of the Board of Directors (the “Board”) of Photronics, Inc. (the “Company”) is established to assist the Board and the Company’s management in fulfilling its oversight responsibilities to the shareholders and investment community by reviewing and reporting on technology based issues as well as cybersecurity risks, protection, and mitigation.

The Committee has the responsibilities and powers set forth in this charter. Management is responsible for the preparation, presentation, and self-assessment of the Company’s IT Systems and the policies and controls governing their use.

In fulfilling its responsibilities, the Committee shall endeavor to maintain free and open communication between the Committee, independent technology audit firms and/or external consultants, and management of the Company.

ORGANIZATION, MEMBERSHIP, AND MEETINGS

1. The Committee shall be comprised of at least one member of the Board of Directors. In addition, the Committee may request that the Company’s Chief Information Technology Officer (“CIO”), and other appropriate Company personnel attend Committee meetings on a regular or periodic basis.
2. Members of the Committee shall be appointed annually by the Board. Members may be replaced by the Board at any time, but shall otherwise serve until a successor has been named.
3. The Committee shall meet at least two times a year, but shall have the authority to convene additional meetings, as circumstances require. The Committee may invite members of management, independent technology audit firms, external consultants, legal counsel or others to attend meetings and to provide relevant information. At least annually, the Committee shall hold an executive session at which only independent directors are present.
4. The Committee may form and delegate authority to subcommittees when appropriate, or to one or more members of the Committee.
5. The Committee may appoint the Chair of the Committee who shall preside at all meetings. At all meetings of the Committee, a majority of the members of the Committee shall constitute a quorum for the transaction of business, and the act of a majority of the members of the Committee present at a meeting at which a quorum is in attendance shall be the act of the Committee. Members of the Committee may participate in any meeting by means of a conference telephone or similar communications equipment by means of which persons participating in the meeting can hear each other and such participation shall constitute presence in person at such meeting.

CYBERSECURITY RISK MANAGEMENT COMMITTEE CHARTER

6. An agenda, together with materials related to the subject matter of each meeting, shall be sent to members of the Committee prior to each meeting. The Committee shall maintain written minutes of its meetings, which minutes will be filed in the corporate minute book. Any person present at a meeting may be appointed by the Committee as Secretary to record the minutes.
7. The Committee may authorize any action by written consent of a majority of its members, including email or other electronic communication.

THE COMMITTEE SHALL

Review and provide high level guidance on technology related issues of importance to the Company, including but not limited to:

1. The Company's technology landscape, competitive assessment and roadmap for future development.
2. The Company's cybersecurity and other information technology (IT) risks, controls and procedures, including high level review of the threat landscape facing the Company and the Company's strategy to mitigate cybersecurity risks and potential breaches. The Committee shall also review the recovery and communication plans for any unplanned outage or security breach.
3. The Company's technology planning processes to support its growth objectives as well as acquisitions and the system integrations required in support of such activities.
4. The integrity of the Company's IT Systems' operational controls to ensure legal and regulatory compliance.
5. Data Management Systems & Processes, including security of the Company's data repositories (US and EU), encryption practices, and third party use of the Company's customers' data.
6. Review the Company's Cyber insurance policies, if applicable, to ensure appropriate coverage and that all insurance terms and conditions are being met.
7. With the assistance of Company management, provide an IT Risk Assessment Report to the Board on an annual basis, including systems and processes relating to cybersecurity.
8. Review the Company's development and training plan for critical IT staff as well as succession planning and employee training of cybersecurity risks.

The Committee shall have the authority to retain outside technical consultants or other appropriate advisors. The Company shall provide for appropriate funding, as determined by the Committee, for payment of compensation to such consultants.

The Committee shall review and reassess the adequacy of this Charter periodically and recommend any proposed changes to the Board for approval.

The Committee shall periodically review its performance.