

# Charter of the Security Committee of the Board of Palo Alto Networks, Inc.

Last updated on August 19, 2026

## Purpose

The purpose of the Security Committee is to assist the Board of Directors (the "**Board**") of Palo Alto Networks, Inc. (the "**Company**") with fulfilling its oversight responsibility with respect to the Company's security of personnel, facilities, information infrastructure and all company information, including data governance, privacy, compliance, cybersecurity and oversight of associated risks and other tasks related to the Company's security functions as the Board may delegate to the Committee from time to time.

## Composition

1. **Membership and Appointment.** The Security Committee shall consist of at least three (3) members of the Board. Members of the Security Committee shall be appointed by the Board upon the recommendation of the Governance and Nominating Committee of the Board and may be removed by the Board in its discretion.
2. **Qualification.** At least a majority of the members of the Security Committee shall meet the independence requirements of the Nasdaq Stock Market and such other qualifications as may be established by the Board from time to time.
3. **Chairperson.** The Board may designate a chairperson of the Security Committee. If the Board does not designate a chairperson, a majority of the members of the Security Committee may elect a chairperson of the Security Committee.

## Responsibilities

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

1. **Security Risk Oversight.** Review and discuss with management (i) the Company's policies, plans, metrics and programs relating to the physical security of the Company's facilities and employees as well as enterprise cybersecurity and data protection risks associated with the Company's security-related infrastructure and related operations, and (ii) the effectiveness of the Company's programs and practices for identifying, assessing and mitigating such risks across the Company's business operations.
2. **Preparedness.** Review and discuss with management (including the chief information security officer) the Company's cyber crisis preparedness, security breach and incident response plans, communication plans, and disaster recovery and business continuity capabilities with respect to the foregoing.
3. **Oversight of Safeguards.** Review and discuss with management (including the chief information security officer) the safeguards used to protect the confidentiality, integrity, availability, safety and resiliency of the Company's employees, facilities, intellectual property and business operations.
4. **Compliance Oversight.** Receive reports from management (including the chief information security officer) on the Company's compliance with applicable information security and data protection laws and industry standards, new or updated legal implications of security, data privacy, and/or other regulatory or compliance risks to the Company or the Company's employees, facilities and business operations and the threat landscape facing the Company and the Company's business operations.
5. **Strategic Oversight.** Review and advise on the Company's physical and cybersecurity strategy, crisis or incident management and security-related information technology planning processes and review strategy for investing in the Company's security systems with the Company's chief product officer and chief information security officer.
6. **Public Disclosure.** Review and discuss with management the Company's public disclosures, including in its reports filed with the Securities and Exchange Commission, relating to the Company's security of its employees, facilities and information technology systems, including privacy, network security and data security.
7. **Outside Partners.** Review and discuss with management (including the chief information security officer) the cybersecurity risks associated with the Company's outside partners (such as vendors, suppliers, operations partners, etc.).

## Meeting and Procedures

1. **Meetings.**
    - The Security Committee will set its own schedule of meetings and will meet at least two (2) times per year, with the option of holding additional meetings at such times as it deems necessary or appropriate. The chairperson of the Security Committee shall preside at, and approve the agenda for, each meeting. If a chairperson is not designated or present, an acting chair may be designated by the Security Committee members present. The Security

Committee may act by written consent (which may include electronic consent), which shall constitute a valid action of the Security Committee if it has been approved by each Security Committee member and shows the date of approval. Any written consent will be effective on the date of the last approval and will be filed with the minutes of the meetings of the Board.

- Written minutes of the Security Committee will be kept and filed with the minutes of the meetings of the Board.
- The Security Committee may invite to its meetings any director, officer or employee of the Company and such other persons as it deems appropriate in order to carry out its responsibilities. The Security Committee may also exclude from its meetings any persons it deems appropriate, including non-management directors who are not members of the Security Committee, in order to carry out its responsibilities.

2. **Reporting to the Board of Directors.** The Security Committee shall report regularly to the Board (i) following meetings of the Security Committee, (ii) with respect to its review and assessment of security matters and such other matters as are relevant to the Security Committee's discharge of its responsibilities and (iii) with respect to such recommendations as the Security Committee may deem appropriate. The report to the Board may take the form of an oral report by the chairperson or any other member of the Security Committee designated by the Security Committee to make such report.

3. **Authority to Retain Advisors.** In performing its responsibilities, the Security Committee shall have the authority to engage and obtain advice, reports or opinions from internal or independent counsel, consultants, and other expert advisors, as it determines necessary or appropriate, to carry out its duties. The Company will provide appropriate funding, as determined by the Security Committee, to pay any outside advisors hired by the Security Committee and any administrative expenses of the Security Committee that are necessary or appropriate in carrying out its activities.

4. **Subcommittees.** The Security Committee may form subcommittees for any purpose that the Security Committee deems appropriate and may delegate to such subcommittees such power and authority as the Security Committee deems appropriate. If designated, any subcommittee will establish its own schedule and maintain written minutes of its meetings, which minutes will be filed with the minutes of the meetings of the Board. The Security Committee shall not delegate to a subcommittee any power or authority required by law, regulation or listing standard to be exercised by the Security Committee as a whole.

5. **Committee Charter Review.** The Security Committee shall review and reassess the adequacy of this charter annually and shall submit any recommended changes to the charter to the Board for approval.

6. **Performance Review.** The Security Committee shall review and assess the performance of the Security Committee on an annual basis.

7. **Access**. The Security Committee shall be given full access to the chairperson of the Board and management, as well as the Company's books, records, facilities and other personnel.