BOARD CYBER AND INFORMATION SECURITY COMMITTEE CHARTER

This Charter is hereby adopted by the Board of Directors (the "Board") of Aboitiz Equity Ventures Inc. (the "Company") to outline the core duties and responsibilities and the basic review processes of the Board Cyber and Information Security Committee (the "Committee").

A. Purpose

The purpose of the **AEV Board Cyber and Information Security (CIS) Committee** is to carry out the responsibilities delegated by the AEV Board in relation to its duty to provide strategic guidance encompassing choices that have a long-term impact on the overall direction, objectives, reputation and competitive advantage of the Group and ensure the establishment of a system of governance (processes, policies, controls, and management) for the Aboitiz Group and its Strategic Business Units ("SBU", collectively the "Aboitiz Group") on matters relating to cyber and information security.

B. Structure

1. Membership

The Committee shall consist of at least three (3) directors. At least one (1) of the members of the Committee must be an independent director, and one (1) member is the Chairman of the Board Risk and Reputation Management Committee.

In the performance of its duties and responsibilities, the Board may appoint external consultants or key officers within the Aboitiz Group who are subject-matter experts to act as ex-officio, non-voting members.

2. Chairman

The Chairman of the Committee will be appointed by the Board and must be a non-executive director of the Board.

3. Term

The members of the Committee shall be appointed by the Board during its annual organizational meeting. Each member shall serve up his or her appointment until the next organizational meeting of the Board unless earlier removed or replaced.

The members of the Board may be removed or replaced, with or without cause, by a majority vote of the directors present in the Board meeting, where there is a quorum. Any vacancy in the Committee shall be filled by a majority vote of the directors present in the Board meeting, where there is a quorum.

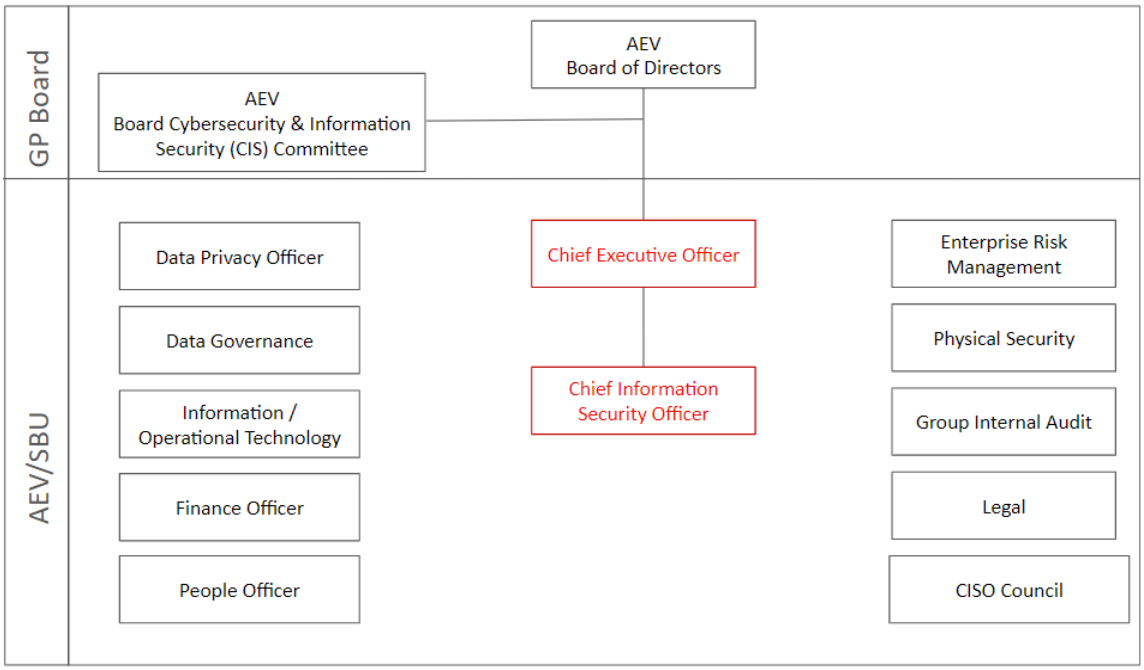

Figure-1. Board Cyber and Information Security Governance Structure

C. Qualifications of the Committee Members

In order for the board members to carry out their functions effectively, they must posses the following qualifications:

1. A practical understanding, knowledge and experience of cybersecurity principles, technologies and best practices for the effective management of cybersecurity risks.
2. Proficiency in assessing and managing cybersecurity risks and well-versed in risk mitigation strategies and incident response planning.
3. Knowledge of relevant cybersecurity regulations and compliance requirements to ensure adherence of the organization to legal and industry standards.
4. A strategic mindset and the ability to align cybersecurity initiatives with the overall business goals and objectives of the organization.
5. Strong leadership skills and effective communication for guiding the organization through cybersecurity challenges and ensuring that cybersecurity-related decisions are well understood at all levels.

6. Skilled in crisis management to be able to effectively respond to cybersecurity incidents and challenging situations.
7. Posses an understanding of emerging cybersecurity technologies and trends to proactively address evolving threats and vulnerabilities.
8. Familiarity with the legal and ethical dimensions of cybersecurity to make informed decisions that uphold the organization's integrity and reputation.
9. A dedication to continuous learning and professional development in the ever-evolving field of cybersecurity to remain effective and relevant as board director.

D. Duties and Responsibilities of the Board

The Board assumes a pivotal role in overseeing the implementation and adherence to the seven (7) guiding principles within our organizational framework that encompass the following:

- Governance & Oversight: The AEV Board has oversight and final approval authority on all strategic decisions related to Group CIS. AEV/SBU shall have a Cyber & Information Security Operating Manual that aligns to the Group CIS Manual of minimum standards, and shall contain policies, controls, standards, implementing guidelines, aligned to the NIST Framework IS27001, industry specific & regulatory standards, and tailored to the needs of the SBU operating environment and risk assessment. Compliance to the Group CIS Manual will be audited annually by the Internal Audit Teams and reported to the Board Audit and CIS Board Committees.

- Collaboration and Communication: The CISO Council, whose member are all the CISOs of AEV/SBUs, will be the venue for collaboration, communication, sharing of internal and external best practices, threat and market intelligence sharing, and review of policies and standards to update AEV/SBU manuals, practices and guidelines.

- Acceptable Use Policy (AUP): The Acceptable Use Policy shall be maintained, reviewed, updated whenever there are changes to policies. Strict compliance to the AUP shall apply to all team members, system owners, authorized third party contractors and stakeholders who have access to systems, information and equipment. Strict compliance shall be embedded in the core operating processes of AEV/SBUs and in the Code of Conduct.

- Cyber Risk Management: Each SBU will use a cyber risk management approach in prioritizing and allocating resources to address its cyber & information security risks. Based on best practices, the CTO and CISO Shall be separate functions. Each SBU shall appoint a CISO, reporting directly to the SBU CEO. The small SBUs will have their CIS heads functionally report to the AEV CISO and may administratively report to the SBU Technology Heads. Any exceptions to this guideline will require approval from the Group CEO.

- Major Incident Response and Crisis Management: Incident response plans should be regularly tested and updated by AEV/SBUs to ensure its effectiveness. Through collaboration, the CISO council is responsible for assisting AEV/SBUs suffering a major incident to mitigate its impact as soon as possible. Internal Audit teams may conduct spot audits on major incidence for proper assessment of facts prior to escalation to Group CEO/AEV Board.

- Training, Awareness & Continuous Improvement: AEV/SBUs will maintain a comprehensive program to address cyber risks and threats for each business, and will continually evaluate, update, enhance its cybersecurity operations to ensure that all standards, guidelines are effective, efficient, and embedded in all business processes.

- Third Party Risk: CIS Teams of AEV/SBUs should ensure protection against third party risks from internal and external individuals and entities e.g. suppliers, customers, partners, team members, by implementing robust programs that provide "always on" vulnerability assessment and mitigation to protect ourselves and other third parties.

This Board diligently monitors the alignment of our operations with these principles, ensuring that our strategic initiatives remain ethically sound, financially prudent, and in compliance with relevant regulations. It is the responsibility of this Committee to act in what it reasonably believes to be in the best interests of the Company, its shareholders, and stakeholders. In discharging that obligation, the Committee has the following authority and responsibilities:

1. Conduct a thorough evaluation and alignment analysis of the Group's cyber and information security programs against industry benchmarks, best practices and overall business objectives, and provide recommendations to the AEV Board regarding strategic decisions that have a long-term impact on the overall direction, objectives, reputation and competitive advantage of the Group.

2. Ensure investments in cyber and information security programs capitalize on opportunities, generate tangible business value, maintain compliance with relevant laws and regulations, and effectively address threats, including those arising from the organization's risk quantification, vulnerabilities, evolving regulatory landscape, industry developments, and technological innovations.

3. Provide oversight on the annual assessment of the potential economic impact of cyber and information security risks to the Aboitiz Group's businesses.

4. Ensure that AEV and each SBU maintains an auditable Cyber and Information Security manual based on the agreed group Cybersecurity minimum standard that aligns with industry best practices and standards.

5. Assess the effectiveness of the Group's data breach incident response and recovery plan, including disclosure, investigation, remediation, and post-breach security measures.

6. Ensure that AEV and each SBU has an adequate training and awareness program that cultivates a security-conscious culture.

7. Cultivate a resilient organizational culture that values agility, innovation, and continuous improvement to be able to effectively steer the organizations through both anticipated and unforeseen challenges, positioning the organization to respond effectively and evolve strategically.

8. Review and approve, at least annually, any amendments or improvements to the Aboitiz Group cyber and information security programs, initiatives, and other related policies.

E. Authorities of the Committee

The Committee shall have the authority to undertake any action as it may deem necessary in the performance of its duties and responsibilities set forth in this Charter. The Committee shall have the following authorities, among others:

1. Consistent with established AEV policies, this Committee's efforts are directed toward AEV and its Managed units where the AEV CISO and AEV Board CyberCom have jurisdiction. This Committee is limited to the cybersecurity principles in Section D above and as established in the Aboitiz Group's Cyber & Information Manual as it relates to AP and UBP with their own CISO and Board Cyber Committees.

2. Periodically receive reports and regular updates from management on relevant matters involving cyber and information security-related concerns, strategies, implementation programs, issues and challenges, and other relevant matters as the Board may deem necessary;

3. Require the attendance of any of the Company's directors, officers, or other employees, or any other persons, whose advice and counsel are sought by the Committee, at 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.

4. Engage, obtain advice, assistance, and authorize investigations into or studies of any matters within the Committee's scope of responsibilities to any internal or external experts, consultants, or other advisors as it deems advisable. Expenses related to the fees of the said experts, consultants, or advisor, shall be approved in accordance with the Company's delegated financial levels of authority.

5. Ensure compliance with regulatory standards and best practices on information security and cybersecurity; and

6. Create and delegate authority to subcommittees as may be appropriate and in accordance with applicable laws or regulations.

F. Meetings of the Board Cybersecurity Committee

1. Frequency of Meetings

The Committee shall formally meet at least four (4) times a year to discharge its duties and responsibilities as outlined herein. In addition to regular meetings, special meetings can be called by the Chairman of the Committee or any two members as required.

2. Notice of Meetings

The notice of the Committee meetings shall be given four (4) weeks prior to the scheduled meeting. Notices for special meetings may be sent at least two (2) business days before the date of the special meeting. Notices may be sent in writing, through electronic mail, or by telefacsimile, among others.

3. Agenda

The Chairman, in consultation with the other members of the Committee, shall propose a list of items to be addressed by the Committee during the year. The Chairman shall ensure that the agenda for each Committee meeting is circulated to each member of the Committee two (2) weeks prior to the meeting and the presentation materials shall be circulated five (5) days prior to the date of the actual meeting in accordance with the existing Board Charter of the Company.

4. Quorum and Voting

A majority of all the members of the Committee present in person or by means of a video-conference, teleconference, or other modes of communication in which all persons participating in the meeting can completely and clearly hear each other

shall constitute a quorum. The members participating in the meeting shall have received the agenda and all the materials for the meeting in accordance with the Board Charter of the Company.

The majority vote of all the voting members shall be required for the Committee to approve, authorize, or take any action.

5. Secretariat

The Office of the Corporate Secretary of the Company and the Office of the Chief Information Security Officer shall jointly act as the secretariat of the Committee.

6. Minutes

All Committee meetings must be duly documented and filed, and shall be maintained with the books and records of the Company. The minutes of the Committee meetings must be available for review and approval not more than five (5) business days after the meeting and for signature at the next committee meeting.

7. Per Diems

The Committee members shall be entitled to per diem for every attendance to a Committee meeting.

G. Reports of the Board Cyber and Information Security Committee

The Chairman of the Committee shall submit to the Board a copy of the reports of the Committee meeting within six (6) calendar days prior to the meeting of the Board and discuss with the Board the highlights of the matters discussed during the Committee meetings.

H. Resources of Board Cyber and Information Security Committee

The Committee may request that any director, officer, or employee of the Company, or other persons whose advice and counsel are sought by the Committee, to attend any of its meetings to provide such pertinent information as the Committee may require.

The Committee has the sole authority to appoint, retain and terminate, as it deems necessary or appropriate, any legal advisor or other consultants, including search firms or other professionals to advise and assist the Committee in fulfilling its duties and responsibilities. The Committee shall approve the fees to be paid as well as the terms of the engagement.

I. Assessment of the Performance of the Committee

The Board shall provide the standards for evaluating the performance and effectiveness of the Committee in fulfilling its duties and responsibilities as set out in this Charter and in the Company's Manual on Corporate Governance.

J. Review of the Committee Charter

The Committee shall review this Charter at least annually and recommend, at the last Committee meeting of the year, any proposed changes to the Board for approval, together with such amendments as it deems necessary and appropriate in order to comply with the legal needs of the Company and any regulatory developments affecting thereto.