This Cybersecurity Committee Charter (the "Charter") was recommended by the Information Technology Committee (ITCom) to the Risk Management Council for adoption across all Aboitiz Group of companies (the "Group").

1.0 PURPOSE

The purpose of this document is to define the Aboitiz Groupwide Cyber Security Committee's mission and authority, governance structure, membership, duties and responsibilities (including those of the committee members), and meetings and procedures.

2.0 SCOPE

This document covers all Strategic Business Units (SBUs), Business Units (BUs) and AEV Corporate Service Units (CSUs) of the Aboitiz Group.

3.0 DEFINITION OF TERMS

3.1 ISMS – Information Security Management System

3.2 CEO – Chief Executive Officer

3.3 MANCOM – Management Committee

3.4 ISMR – Information Security Management Representative

3.5 SBU – Strategic Business Unit

3.6 BU – Business Unit

3.7 CSU – Corporate Service Unit

3.8 ISMS – Information Security Management System

Process Owner	Document Created By	Reviewer/s	Approver/s
Charmaine Valmonte	Charmaine Valmonte – 12/06/2019	Jose Grego Sitoy – 12/12/2019 Ricardo Lacson – 12/12/2019 Christine Kempeneers – 12/12/2019 Risk Management Steering Committee – 12/12/2019	Risk Management Council Chairman – 12/12/2019 Annacel Natividad – 12/12/2019

3.9 ISMR – Information Security Management Representative

3.10 Cybersecurity: The ability to protect or defend the use of cyberspace from cyber attacks. It is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises **cybersecurity** and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems.
Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
availability, which means ensuring timely and reliable access to and use of information.
safety and reliability of systems supporting operational technology

4.0 MISSION

4.1 The mission of the Cybersecurity Committee (the "Committee") under the ITCom is to enhance the Aboitiz Group's understanding and oversight of systems, including processes, policies, controls and procedures in accordance with the Aboitiz Group Wide Information Security Management Policy (AGW-ISM-PL-001) to:

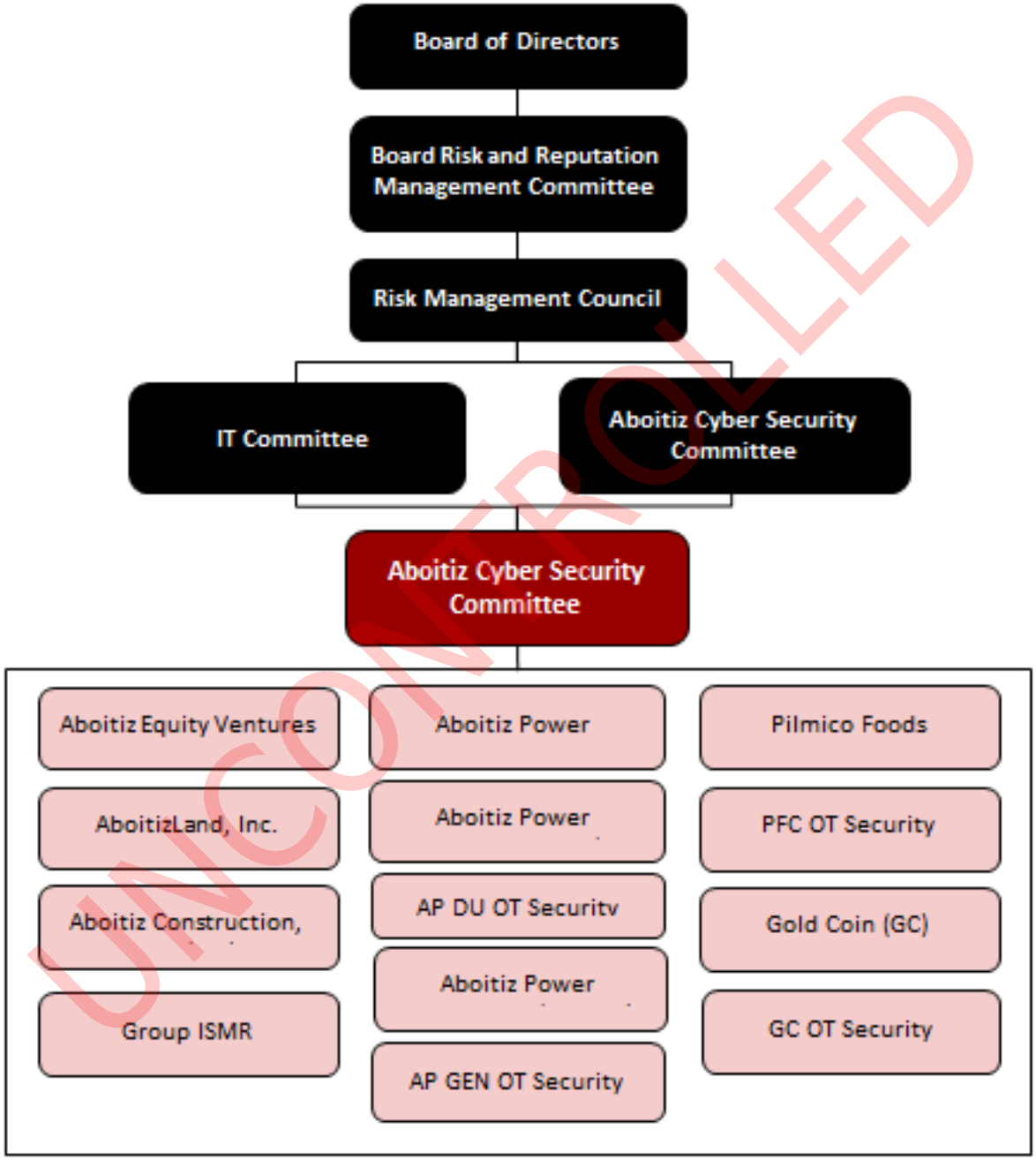
4.1.1 assess, safeguard and mitigate the Group's key cybersecurity, information technology (IT) and operational technology (OT) risks against both internal and external threats;
4.1.2 ensure adequate protective systems are in place against security breaches which can effectively safeguard the Group's IT and OT infrastructure, assets, intellectual property, development environment as well as the Group's data to include customer and other third party confidential information in the Group's possession or custody;
4.1.3 ensure the integrity of security in any of the Group's products and services that collect, process and/or handle confidential data;
4.1.4 develop and monitor the integrity of the Group's IT/OT systems and controls to ensure legal and regulatory compliance over data security;
4.1.5 respond to and manage cybersecurity threats, including data breach incidents and;
4.1.6 ensure business continuity in the event of cybersecurity incidents on any of the Group's IT/OT systems.

4.2 COMMITTEE AUTHORITY

4.2.1 The Committee shall have the authority to undertake any other action or exercise such other powers, authority, and responsibilities as the Committee determines necessary or appropriate to the discharge of the responsibilities and duties set forth in this Charter.
4.2.2 The Committee shall have full access to the books, records, facilities, and personnel of the organization.
4.2.3 The Committee may expense, obtain advice, assistance, and support from outside advisors as it deems appropriate to perform its duties. Subject to applicable laws, regulations or rules.
4.2.4 The Committee may delegate authority to members of management and also form and delegate authority to subcommittees consisting of one or more members, when it deems appropriate. In so delegating authority, the Committee shall not absolve itself from the responsibilities it bears under the terms of this Charter.

5.0 GOVERNANCE STRUCTURE

5.1 The governance structure is as follows:



5.2 RELATIONSHIP WITH OTHER COMMITTEES

This document is aligned with the Aboitiz Groupwide Information Security Management Policy (AGW-ISM-PL-001)and shall make reference to both the Board Risk and Reputation Management Committee Charter and Aboitiz Groupwide ISMS Charter. The roles and responsibilities relevant to the implementation of cybersecurity across the Aboitiz Group are stipulated within this document.

5.2.1 Information Technology Committee (ITCom)
5.2.1.1 Composed of the SBU/BU IT Heads and the Cybersecurity Committee Chair.
5.2.1.2 Responsible for developing a medium to long term Group IT Strategy and Plan which includes direction setting, organizational development, technology investment and resource management aligned to the Aboitiz Group Information Security Requirement.
5.2.1.3 Acts as a clearinghouse for enterprise applications and major SBU/BU Technology Projects with reference to cybersecurity.
5.2.2 Digital Committee (DIGICOM)
This Committee defines the overall strategic direction and innovations in terms of digital transformation including related services and business acquisitions.

6.0 MEMBERSHIP

6.1 This Committee shall be composed of a maximum of 2 duly selected representatives per Strategic Business Unit (SBU) or Business Unit (BU) under the Group including the Group ISMR. Each representative is deemed to have experiential credentials that would help in addressing matters specifically delegated to the Committee by ITCom.

6.2 The Chairperson of this Committee (the "Chair") as appointed by the ITCom is the Vice President for IT Security, Compliance and Quality Assurance of Aboitiz Equity Ventures Inc. Committee members may be removed from the Committee, with or without cause, by the ITCom. Any action duly taken by the Committee shall be valid and effective, whether or not the members of the Committee at the time of such action are later determined not to have satisfied the membership requirements provided herein.

7.0 DUTIES AND RESPONSIBILITIES

7.1 The Committee's duties and responsibilities shall include, without limitation, the following:
7.1.1 Work with senior management to understand the Group's cybersecurity risks, including the potential likelihood, frequency, and severity of cyberattacks and data breaches.
7.1.2 Develop the governing body consistent with the IT and Information Security Standards, Policies and Strategies and its review thereof.
7.1.3 Discuss cybersecurity policies as to risk assessment and risk management, including the review of the guidelines and policies established by the Company to assess, monitor, and mitigate the Company's significant cybersecurity risk exposures.
7.1.4 Oversee activities related to cyber risks, such as reviewing adequacy of the cyber risk budget, assessing the effectiveness of security programs and top-level policies; assessing roles, responsibilities, and reporting relationships for privacy and security issues; and ensuring development and adequacy of an incident response plan and adequacy of resources to respond to a breach.
7.1.5 Review significant cybersecurity investments and expenditures and make recommendations, where appropriate.
7.1.6 Receive, as and when appropriate, reports, and recommendations from management regarding, among other things, cybersecurity breaches and cybersecurity risks.
7.1.7 Make such recommendations to the ITCom and management with respect to any of the above and other matters as the Committee deems necessary or appropriate.
7.1.8 Regularly report the status of cybersecurity risk management of the Group to key stakeholders.

7.2 The Cybersecurity Committee functional members' specific roles and responsibilities shall include, without limitation, the following:
7.2..1 IT Security
7.2.1.1 Lead by the IT Security, Compliance and Quality Assurance Office, responsible for the overall oversight of the group-wide cybersecurity program and liaises with the various SBU/BU

ISMRs as applicable.
7.2.1.2 Reviews, monitors and reports implementation progress of groupwide ISMS implementation during the regular Risk Management Steering Committee Meetings/Reviews.

7.2.2 SBU IT/OT Security
7.2.2.1 Has overall accountability for leading and overseeing the cybersecurity implementation at SBU/BU Level
7.2.2.2 Liaises / communicates with SBU/BU IT Head in implementing IT/OT Security Technical Controls aligned to information security requirements
7.2.2.3 Regularly evaluates the effectiveness of the technical and operational controls in addressing information security risks identified.

7.2.3 The SBU/BU IT Head is accountable for implementing IT/OT Security Technical Controls based on the information security requirements within the Aboitiz Group in coordination with the SBU/BU ISMS Lead.

8.0 MEETINGS AND PROCEDURES

8.1 The Chairperson of this Committee (the "Chair") as appointed by the ITCom is the Vice President for IT Security, Compliance and Quality Assurance of Aboitiz Equity Ventures Inc. Committee members may be removed from the Committee, with or without cause, by the ITCom. Any action duly taken by the Committee shall be valid and effective, whether or not the members of the Committee at the time of such action are later determined not to have satisfied the membership requirements provided herein.

8.2 The Chair (in her or his absence, a member designated by the Chair) shall preside at each meeting of the Committee. The Committee shall have the authority to establish its own rules and procedures for notice and conduct of its meetings as long as it does not contravene with the provisions set by the ITCom.

8.3 The Committee shall meet monthly prior to the IT Committee's monthly meeting.

8.4 The Chair, in consultation with the other committee members, shall determine the schedule, length of the meetings and agenda for the Committee meetings. The Chair shall appoint a committee member to take the minutes of the meetings and will be responsible for the distribution of these minutes accordingly.

8.5 Attendance on meetings by one-third of the members serving on the Committee, but not less than two members, shall constitute a quorum for the transaction of business for these meetings.

8.6 Non-management directors who are not members of the Committee may attend and observe meetings of the Committee, but shall not participate in any discussions unless invited to do so by the Committee, and in any event, shall not be entitled to vote.

8.7 The Committee may, at its discretion, include in its meetings, members of the Group's management, or any other person whose presence the Committee believes to be desirable and appropriate. On the other hand, the Committee may also, at its discretion, exclude from its meetings any person it deems inappropriate, including but not limited to any non-management director who is not a member of the Committee.

8.8 The Chair shall report the recommendations, deliberations, and actions of the Committee at the meetings of the ITCom and/or Risk Management Steering Committee, or other additional occasions as deemed appropriate by the Group's management.

8.9 The Cybersecurity Committee shall evaluate the performance of the committee and its members at least annually. The results shall be communicated to the ITCom.

9.0 AMENDMENT OF CHARTER

DR No:DR-2021-027, Issued by DCS on 04/27/2021

The Cybersecurity Committee shall review and assess the adequacy of the charter at least annually, and any proposed changes shall be forwarded to the ITCom for endorsement to the Risk Management Council for approval.

REVISION HISTORY

Version	Description of Changes	Effective Date
1	First Issue	January 7, 2020