ACPSEM Policy for the Management of Cyber Security

1. Policy Principles

This policy is written with an understanding that cyber security and data fraud is a growing risk for all businesses with governance, insurance, operational, and reputational implications. It is also cognisant of the scale and characteristics of the ACPSEM's operations, including a reliance on the sound understanding and management of cyber risk by multiple vendors (2) of cloud-based services and an outsourced IT management function.

Additionally, the policy is cognisant of the requirements of the 2018 National Notifiable Data Breach Scheme (Australia) and notes that there is currently no similar legislation in NZ, though it is expected in 2020.

2. Responsibilities of the ACPSEM Board

1. It is the responsibility of the ACPSEM Board to understand what data ACPSEM systems hold, how it is protected, and whether the College has adequate arrangements in place to ensure business continuity and cyber remediation.
2. The Board has a role in the response to any cyber breach that may occur in that it needs to ensure that a remediation process is in place, ready to be activated; and at the time of a cyber breach, have sufficient trust in the process -preparation, planning and training – undertaken by staff and the third party vendors to manage cyber incidents.
3. The Board must require of staff that it monitor and report on the cyber security measures put in place by its vendors on an annual basis or as otherwise required by the Board.
4. The Board should ensure that, should a breach occur, communication to members, other persons enrolled in programs, stakeholders and regulators is open, transparent and honest.

3. Responsibilities of the ACPSEM CEO

Accountability for achievement of all Board Responsibilities listed at 1 to 4 above is delegated to the ACPSEM CEO.

IN additional to the annual reporting mechanism specified in 2 above, the CEP shall ensure that the occurrence of any cyber breach is noted in ACPSEM Board Agenda Papers.

Cyber breaches will also be recorded in a Register of Cyber Events that can be viewed by the Board at any time.

4. Cyber Security Management Requirements

1. The ACPSEM recognises the need to have a clear understanding of the cyber risk to which it is exposed and to prepare, plan, and train in a manner commensurate with the risks identified.
2. The ACPSEM recognises the need to have a clear understanding of:
    a. The value of its data
    b. Who has access to its data,
    c. An accurate understanding of how data is held and managed in the private cloud systems it uses; and
    d. Howe and how well data is being protected
3. The ACPSEM recognises the importance of preparing for cyber events rather than reacting under duress, and that preparation includes Board discussion and staff readiness (such as simulation) activities.
4. The ACPSEM recognises that short term technical cyber breaches may also have other longer-term impacts on individuals and company reputation and that these potential impacts should be considered in preparation, planning and training.

Authorised by	ACPSEM Chair
Authorised on	27 October 2019
Effective date	27 October 2019
Review date	327 October 2022
Responsible officer	ACPSEM CEO
Enquiries	N/A
Version	1.0
Policy Domain	PSB

Document History

Version	Date	Author	Reason
1.0	October 2019	Sharon Flynn	First draft