Annexure A – Medibank's cybersecurity and information security framework

Policy framework

Medibank had, at least, the following cybersecurity or cybersecurity-related policies and standards in place from the dates specified:

1 Enterprise Security Policy (version 6.3), effective from November 2017.

2 Information Security Policy (version 7.0) (sets out Medibank's Information Security Documentation Framework), effective from 1 May 2021.

3 Information Security Policy (version 7.1) (sets out Medibank's Information Security Documentation Framework), effective from 26 May 2022.

4 Enterprise IT Security Principles, effective from November 2017.

5 Enterprise Security - Vulnerability Management Standard (version 1.6), dated November 2017.

6 Enterprise Security - Vulnerability Management Standard (version 1.7), effective from 1 September 2021.

7 Enterprise Security - Vulnerability Management Standard (version 2.0), effective from 1 January 2022.

8 Enterprise Security Access Control Standard (version 2.10), approved in April 2020.

9 Enterprise Security Anti-Malware Standard, approved in May 2019.

10 Enterprise Security Audit Logging Standard, approved in May 2020.

11 Enterprise Security Standard - Backup and Recovery (version 1.6), approved in November 2017.

12 Enterprise Security Standard - Cryptographic Controls (version 1.6), approved in November 2017.

13 Enterprise Security Standard - Network Design (version 1.7), approved in November 2017.

14 Enterprise Security Standard - System & Software Development (version 1.6), approved in November 2017.

15 Bring Your Own Mobile Device Policy (version 2.3), effective from December 2017.

16 Information Security BYOD Policy (version 1.0), effective from 13 September 2022.

17 Information Security Password Standard (version 1.0), effective from September 2021.

18 Enterprise Security Suppliers & Partners Standard (version 1.7), approved in September 2019.

19 Information Security Supplier Management Standard (version 2.0), approved in March 2022 and effective from April 2022.

20 IT&T Acceptable Use Policy (version 5.0), effective from May 2020.

21 IT&T Acceptable Use Policy (version 6.1), effective from 1 August 2021.

22 Medibank Zero Trust Strategy (version 1.0) dated 13 December 2021.

23 MPL Information Security Temporary Exemption Procedure (version 1.0) dated May 2020.

24 Notifiable Data Breach Reporting Policy dated 7 June 2022.

25 Third-Party Information Security Risk Management Framework (version 1.01), effective from 10 June 2021.

26 Third-Party Information Security Risk Management Procedure (version 1.01), effective from 10 June 2021.

27 Third-Party Information Security Risk Management Roles and Responsibilities (version 1.1) dated 30 March 2021.

28 User Access Audit Policy and embedded IM User Access Audit Runsheet dated 2 December 2020.

29 Crisis Management Quick Reference Guide dated 20 September 2022.

30 IT Security Incident Response Plan and Playbooks (version 1.0), approved 19 September 2022.

31 Operational Risk and Compliance Incident Management Procedure (version 3.1), approved 14 October 2020.

In addition, during the Relevant Period, Medibank had the following policy and standard documents which were not specific to cybersecurity risks from the dates specified below:

32 IT Service Management – Change Management Process (version 1.8) dated 27 January 2021.

33 IT Service Management – Change Management Process (version 1.9) dated 21 January 2022.

34 IT Service Management – Change Management Process (version 1.10) dated 28 September 2022.

35 IT Service Management – Configuration Management Process (version 1.3), covering the period of May 2020 to April 2021.

36 IT Service Management – Configuration Management Process (version 1.4) dated 9 April 2021.

37 IT Service Management – Configuration Management Process (version 1.5) dated 7 June 2021.

38 IT Service Management – Incident Management Process (version 1.6) dated 24 January 2022.

39 IT Service Management – Problem Management Process (version 1.5) dated 21 December 2021.

40 IT Service Management – Request Management Process (version 1.2) dated 12 July 2017.

41 IT Service Management – Service Catalogue Management Process dated 15 August 2017.

42 Procurement Policy, effective from 10 January 2022.

43 Procurement Policy, effective from 20 April 2022.

44 Risk Management Procedure, effective from 30 August 2020.

45 Risk Appetite Statement Policy (version 4), effective from 1 April 2022.

Resources

During the Relevant Period:

46 Medibank's core IT security function comprised a team of 13 full-time IT security professionals.

47 Medibank's FY22 information technology budget was approximately $4-5 million, of which $1 million was allocated for cyber security.