Australian Payments Network

Issuers and Acquirers Community

Device Approval Process Revised 2024

Version 0.1

Issuers and Acquirers Community Device Approval Process

Revised 2024 Version No: 0.1
Effective: 1 January 2025

Table of Contents

Change History

Version	Effective Date	Change
0.1	01/01/2025	Device Approval Process (Revised)

PART 1 INTRODUCTION

1.1 Operation

This document sets out the Australian Payments Network's (the Company) process for approval of Devices, Solutions, and Non-Standard Technologies.
This document operates as follows:

(a) It replaces the Device Approval Process introduced December 2021.

(b) It does not form part of the IAC Code Set and may be varied by the Chief Executive Officer without the need to obtain the approval of the IAF or any other person.

(c) By submitting an approval application or a delta approval application, a Device Approval Applicant agrees to comply with the applicable terms of this document as in force on the date the application was lodged and, where relevant, ensure the Vendor (or any other relevant third party) provides any necessary information and cooperation required for the Device Approval Process.

1.2 Interpretation

(a) The words defined in IAC Code Set - Interpretation and Definitions have the same meaning in this document unless a contrary intention appears. Where there is an inconsistency between a definition reproduced below and a definition in the IAC Code Set, the IAC Code Set definition will prevail. The following definitions are reproduced from the Code Set:

(i) "**Accepted Standards**" means the standards for payment acceptance, transfer of keys or processing of cryptographic data listed in the Device Approval Process.

(ii) "**Approval Period**" means the period during which an Approved Device can be deployed and used in the IAC as provided in the Device Approval Process.

(iii) "**Approved Device**" means a Device that is approved for use within the IAC in accordance with Part 3 of the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management);

(iv) "**Approved Standards Entity**" means an organisation recognised by the Company which develops, maintains and publishes Accepted Standards and lists Devices which have been validated against an Accepted Standard

(v) "**AusPayNet-Approved Devices List**" means the list of Devices approved by the Company and published on the Company's website.

(vi) "**Device**" means a Secure Cryptographic Device, Solution or Non-Standard Technology used for payment acceptance, transfer of keys or processing of cryptographic data.

(vii) "**Device Approval Applicant**" means the applicant seeking approval of Non-Standard Technology in accordance with the Device Approval Process.

(viii) "**Device Approval Process**" means the process for approval of Devices published by AusPayNet on its website.

(ix) "**Letter of Approval**" means a letter, issued by the Company, approving the use of a Device within the IAC or any other notification of device approval contemplated in the Device Approval Process.

(x) "**Non-Standard Technology**" means technology for payment acceptance, transfer of keys or processing of cryptographic data that by nature of its design is unable to meet an Accepted Standard.

(xi) "**Solution**" means the product and/or service used for payment acceptance, transfer of keys or processing of cryptographic data that requires multiple components for the overall product and/or service to meet all applicable security requirements.

(xii) "**Sunset Period**" means the period during which an Approved Device that had been purchased during the Approval Period may be deployed and may continue to be used in the IAC after its approval expires as provided in the Device Approval Process.

(b) Words that are capitalised but not defined in IAC Code Set - Interpretation and Definitions have the following meaning:

(i) **Delta Application** means an application for updating the approval of an Approved Device

(ii) **Documentation Pack** means the system documentation, scheme reports, other laboratory reports, internal testing results and any other documents requested by the Company under the Structured Risk Assessment Process.

(iii) **End of Life** means the date a Device is no longer supported by its vendor.

(iv) **Expired Device** means a device that has reached its expiry date.

(v) **Expired Devices List** means the list published on the Company's website of AusPayNet Approved Devices that have passed their expiry date.

(vi) **NST Process** means the Company's approval process for Non-Standard Technology applicable prior to the introduction of the Structured Risk Assessment Process.

(vii) **Pilot** means deployment for a defined period of time and subject to certain conditions detailed in a Pilot Letter of Approval for Non-Standard Technology.

(viii) **Pilot Letter of Approval** means a letter, issued by the Company, detailing the terms and conditions of the Pilot.

(ix) **Pilot Sponsor** means the Acquirer who agrees to sponsor a Device Approval Applicant during a Pilot.

(x) **Revoked Devices List** means the list published on the Company's website of Approved Devices that have had their approval revoked by the Company.

(xi) **Schedule of Sunset Dates** means the list of Sunset Dates published on the Company's website.

(xii) **SRA** means a structured risk assessment undertaken as part of the Structured Risk Assessment Process.

(xiii) **SRA Questionnaire** means the request for information provided by the Company to the Device Approval Applicant under the Structured Risk Assessment Process.

(xiv) **Structured Risk Assessment Process or SRA Process** means the process outlined in Part 4 for evaluating Non-Standard Technologies.

(xv) **Vendor** means a Device manufacturer or developer.

PART 2 APPROVED DEVICES AND PERIOD OF PERMITTED USE

2.1 Approved Devices

(a) A Device is approved for use in the IAC if the Device is:

(i) listed as approved on the website of an Approved Standards Entity and complies with the requirements in cl 2.2 below; or

(ii) listed in the AusPayNet-Approved Devices List published on the Company's website as detailed in cl 2.3 below; or

(iii) approved for use in a pilot under a Pilot Letter of Approval issued by the Company as detailed in cl 2.4 below.

2.2 Accepted Standard Approved Device

(a) A Device listed as approved on the website of an Approved Standards Entity is approved for use in the IAC if:

(i) the Device complies with an Accepted Standard listed in paragraph (b) below; and

(ii) the Company has not revoked approval of the Device as provided in clause 3.1 below.

(b) A Device listed as approved on the website of an Approved Standards Entity must comply with at least one of the following **Accepted Standards** (including all published annexures) and the **applicable criteria** where specified below to be approved for use in the IAC:

(i) Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements;

(ii) Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Modular Security Requirements;

(iii) Payment Card Industry (PCI) Contactless Payments on COTS (CPoC) Security and Test Requirements;

(iv) Payment Card Industry (PCI) Software-Based PIN Entry on COTS (SPoC) Security Requirements;

(v) Payment Card Industry (PCI) Software-Based PIN Entry on COTS (SPoC) Test Requirements.

(vi) Payment Card Industry (PCI) Mobile Payments on COTS (MPoC) Security and Test Requirements.

Applicable criteria: Compliance with the Accepted Standard extends only to validated MPoC Solutions; it does not extend to MPoC Software, MPoC Service or any other listed components.

(vii) National Institute of Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 140-2 and 140-3.

Applicable criteria: Compliance with the Accepted Standard extends only to HSMs approved by the NIST Cryptographic Module Validation Program (CMVP) at Level 3 or Level 4.

2.3 AusPayNet-Approved Device

(a) A Device listed in the AusPayNet-Approved Devices List is approved for use in the IAC.

(b) A Device will be listed in the AusPayNet-Approved Devices List if:

(i) the Device is approved following the Structured Risk Assessment Process for Non-Standard Technology detailed in Part 4 below; or

(ii) the Device was approved by the Company under a previous NST Process; and

(iii) the Company has not revoked approval of the Device as provided in clause 3.1 below.

2.4 Pilot Approved Device

(a) AusPayNet may approve for use in a pilot a Non-Standard Technology.

(b) The conditions for use in the IAC and term of approval of the Device, are set out in the Pilot Letter of Approval.

2.5 Period of Permitted Use of Approved Devices

(a) An Approved Device is permitted to be used in the IAC subject to Part 3 below, during:

(i) an Approval Period when the Approved Device may be deployed and used in the IAC; and

(ii) a Sunset Period when an Approved Device that had been purchased during the Approval Period may be deployed and may continue to be used in the IAC.

(b) For a Device listed as approved on the website of an Approved Standards Entity and complying with the requirements in clause 2.2 above, subject to Part 3 below:

(i) the Approval Period expires on the expiry date for the Approved Device published on the Approved Standards Entity's website;

(ii) the Sunset Period expires on the sunset date published in the Schedule of Sunset Dates; and

(iii) use of the Device in the IAC must be discontinued before the expiry of the Sunset Period.

(c) For a Device listed in the AusPayNet-Approved Devices List subject to clause 3.1 below:

(i) the Approval Period expires on the expiry date for the Approved Device published in AusPayNet-Approved Devices List following which the Device will be transferred to the AusPayNet Expired Devices List;

(ii) the Sunset Period expires on the sunset date published in the Schedule of Sunset Dates and in the AusPayNet Expired Devices List; and

(iii) use of the Device in the IAC must be discontinued before the expiry of Sunset Period unless a renewal is granted under clause 3.2 below.

(d) For Devices approved under a Pilot Letter of Approval subject to clause 3.1 below:

(i) the Approval Period expires on the expiry date stated in the Pilot Letter of Approval; and

(ii) there is no Sunset Period: use of the Approved Device must be discontinued before the expiry of the Approval Period unless a renewal is granted under clause 4.7(c) below.

PART 3 REVOCATION AND RENEWALS

3.1 Revocation

(a) The Company may conduct periodic assessments of any Approved Device as and when the Company (in its absolute discretion) deems appropriate having regard to changes in security technology, applicable standards, security threats and/or other knowledge of security issues.

(b) An Approved Device may be revoked by the Company prior to expiry of the Approval Period or the Sunset Period if:

(i) approval of the Device is revoked by an Approved Standards Entity;

(ii) the Device is unable to support a security feature required by the IAC; or

(iii) the vendor has determined that an Approved Device has reached End of Life; or

(iv) the Company assesses (in its absolute discretion) that an Approved Device is compromised or is vulnerable to a significant security threat where a timely remediation cannot be provided and determines that the Approved Device should no longer be approved for use in the IAC.

(c) If the Company revokes an Approved Device prior to expiry of the Approval Period or the Sunset Period:

(i) for a Device listed as approved on the website of an Approved Standards Entity, the Company will list the Device on the Revoked Devices List including the date of revocation and notify all members;

(ii) for a Device listed in the AusPayNet-Approved Devices List, the Company will move the Device to the Revoked Devices List and note the date of revocation, notify the Device Approval Applicant in writing of the reasons for its decision and notify all members; and

(iii) for a Device approved under a Pilot Letter of Approval, the Company will notify the Device Approval Applicant in writing the date of termination of the pilot and the reasons for its decision.

3.2 Renewal process for Device listed in the AusPayNet-Approved Devices List

(a) Prior to expiry of the Approval Period, the Company may in its sole discretion:

(i) extend the Approval Period for a period of five years or such other period as the Company deems appropriate having considered the current security landscape, security threats and risk exposures; or

(ii) require the Approved Device be evaluated under the SRA Process in Part 4 below before determining if an extension of the Approval Period will be granted.

(b) If the Approval Period is extended, the Company will:

(i) update the AusPayNet-Approved Devices List with the new expiry date; and

(ii) send the Device Approval Applicant an updated Letter of Approval including the new Approval Period.

PART 4 PROCESS FOR APPROVAL OF NON-STANDARD TECHNOLOGY

4.1 Operation of this clause 4

A Device Approval Applicant may apply to the Company for approval to use a Device that does not comply with an Approved Standard in clause 2.2 above.

The Device Approval Applicant may be an Acquirer, Third Party Provider, Device manufacturer or any other party.

4.2 Application for Approval via the Structured Risk Assessment Process.

The Device Approval Applicant must submit to the Company via email (PAG@auspaynet.com.au) an Application for Approval.

4.3 Structured Risk Assessment Process

Subject to clause 4.5 below, if the Application for Approval is complete, the Company will undertake the Structured Risk Assessment Process outlined in this clause.

The SRA contains the following stages:

(a) Identification

(i) The Company issues to the Device Approval Applicant an SRA Questionnaire.

(ii) Upon receiving the completed SRA Questionnaire, the Company identifies, and then requests from the Device Approval Applicant, a Documentation Pack, listing the information required by the Company to undertake an SRA, together with a Vendor Consent and a Non-Disclosure Agreement.

(b) Review

Following receipt of the documentation the Company will review the material provided. Questions raised during this review will be discussed with the Applicant or their chosen representative.

(c) SRA

The Company will undertake a risk analysis and produce an Assessment Report. The risk analysis will consider the following aspects:

(i) Gaps between the product/solution and related security standards

(ii) Quality of evidence provided and any gaps to expected evidence

(iii) General security risks associated with the solution

(d) Decision

The Company will determine on the basis of the Assessment Report whether the Device should be:

(iv) Approved

(v) Approved with Conditions

(vi) Approved for Pilot

(vii) Declined.

4.3.1 *Application for Approval and SRA Questionnaire*

(i) Every Application for Approval via the Structured Risk Assessment submitted in accordance with the Device Approval Process will be reviewed by the Company.

(ii) If the Application for Approval is complete, the Company will issue to the Device Approval Applicant an SRA Questionnaire.

(iii) The Device Approval Applicant must complete the SRA Questionnaire and forward it to the Company to enable the Application for Approval to proceed.

4.3.2 *Document Pack, Vendor Consent and Confidentiality Agreement*

(i) The Company will review the completed SRA Questionnaire and determine what documentation is required to undertake the SRA including, as appropriate, a letter of approval from other regions, scheme letter of approvals, scheme testing reports, other testing reports or any other document (**Documentation Pack**).

(ii) The Device Approval Applicant must submit:

(A) all documents identified in the Documentation Pack;

(B) the Vendor's Consent (in such form as required by the Company from time to time); and

(C) a Confidentiality Agreement (in such form as required by the Company from time to time).

(iii) These documents must be returned to the Company within four months from the date the Company issues them.

(iv) If the documents required are not received by the Company within that time, the Application for Approval will lapse unless the Company has granted an extension or a waiver (in its absolute discretion).

(v) Following any lapse in an Application for Approval, the Device Approval Applicant must submit a new Application for Approval under the Device Approval Process if it wishes to recommence the application process.

4.3.3 *Review*

(a) The Company will analyse the SRA Questionnaire and Documentation Pack to determine the:

(i) system components;

(ii) vulnerabilities;

(iii) applied mitigants;

(iv) data asset flow; and

(v) any other information relevant to the assessment of the Non-Standard Technology.

(b) The Company will review the SRA Questionnaire and the Documentation Pack. Questions arising during the review will be discussed with the Applicant via email, face-to-face meetings, video conference or other methods as appropriate.

(c) Following the Review, the Company may issue the Device Approval Applicant with a request for additional documentation. The Device Approval Applicant must respond to the Company's request within two months to enable the Application for Approval to proceed.

4.3.4 *SRA*

(a) The Company or a third party nominated by the Company will perform a risk assessment.

(b) The Company will determine the compliance and security risks as part of the structured risk assessment focusing on exposure of sensitive data.

4.3.5 *Assessment Report*

(a) The Company will produce an Assessment Report identifying individual risks and an overall SRA Risk Rating.

(b) The Company will determine the SRA Risk Rating based on an assessment of the totality of exposure calculations, considering the types of exposures disclosed and the scalability of risk, and a consideration of the risk rating principles in Table 1 below.

Table 1 Risk Rating Principles

Risk Ratings	Guiding Principles
Low	1. Data assets are not exposed to known vulnerabilities. 2. Gaps to relevant standards have minimal security impact 3. Mitigations for system components vulnerabilities are mitigated appropriately. 4. Mitigations are verified by third party testing.
Medium	1. Data assets are exposed to some vulnerabilities. 2. Gaps to relevant standards have modest security impact 3. System component vulnerabilities are not adequately mitigated. 4. Data assets are exposed to non-scalable vulnerabilities. 5. System component vulnerabilities are subjected to complex attacks with limited data asset exposure.
High	1. System component vulnerabilities are subjected to non-complex attacks. 2. Significant gaps compared to relevant existing standards 3. Data assets are exposed to scalable vulnerabilities. 4. Compromise of data assets will lead to a significant scale of fraud.

4.3.6 *Low risk assessment*

If the Company determines on the outcome of the SRA that the Device is low risk the Company will:

(a) accept the Device for approval;

(b) send to the Device Approval Applicant a Letter of Approval in accordance with clause 4.4 below; and

(c) publish the Approved Device on the AusPayNet-Approved Devices List.

4.3.7 *Medium risk assessment*

If the Company determines on the outcome of the SRA that the Device is medium risk:

(a) the Company may accept the device for approval with conditions and will:

(i) send to the Device Approval Applicant a Letter of Approval in accordance with clause 4.4 below detailing the applicable conditions; and

(ii) publish the Approved Device on the AusPayNet-Approved Devices List; or

(b) where the SRA Assessment Report identifies security vulnerabilities, provided the Acquirer is the Device Approval Applicant or the Acquirer agrees in writing to be appointed as Pilot Sponsor, the Company may accept the Device on a pilot basis and will send the Device Approval Applicant and Pilot Sponsor, where appointed, a Pilot Letter of Approval detailing the pilot conditions as described in clauses 4.4(c) and 4.6 below.

4.3.8 *High risk assessment*

If the Company determines, on the SRA Assessment Report, that the Device is high risk, the Company will decline the Application for Approval in accordance with clause 4.4(d) below.

4.3.9 *Timing*

The Company will endeavour to complete the SRA Process within two months from receipt of all the documentation referred to in clause 4.3 above. The actual timing will depend on the time the Device Approval Applicant takes to respond to requests for information from the Company, the complexity of the solution, and the quality of documentation received.

4.3.10 Costs

(a) *The Device Approval Applicant agrees to pay reasonable external costs associated* with the device evaluation.

(b) The Company will determine what external costs are required. These costs may include technical security consulting and system testing by a specialised testing company. The Company will provide an estimate of any such costs and the Device Approval Applicant must accept the costs in writing prior to the Company incurring them.

(c) If the Device Approval Applicant does not agree with the Company's determination of the external costs required or the estimate of external costs, the Device Approval Applicant can request a review under Part 5 below.

4.4 Notification of decision and publication

(a) The Company will notify the Device Approval Applicant in writing of its decision.

(b) If the Company approves a Device, the Company will issue a Letter of Approval to the Device Approval Applicant, in a form to be determined by the Company, but such letter will contain at a minimum:

(i) the name of the Device Approval Applicant;

(ii) the Approved Device;

(iii) the approval date;

(iv) the Approval Period which will be five years from the approval date or such other period as set out in the Letter of Approval; and

(v) the conditions, if any, associated with the approval; and

(vi) publish on the AusPayNet-Approved Devices List, the Approved Device, setting out the minimum details contained in the Letter of Approval.

(c) If the Company approves for Pilot a Device, the Company will issue a Pilot Letter of Approval to the Applicant and the Pilot Sponsor where appointed, detailed in clause 4.6 below, but such letter will contain at a minimum:

(i) the name of the Device Approval Applicant;

(ii) the name of the Acquirer;

(iii) the Device identifiers (model name, hardware version, firmware version, application version or other details as appropriate);

(iv) the security vulnerabilities identified in the SRA Assessment Report that are required to be mitigated before the technology can be approved for pilot;

(v) the Approval Period of the Pilot; and

(vi) the conditions of the Pilot including the liability shift to the Acquirer under clause 4.6.3 below in accordance with the Structured Risk Assessment Process.

(d) If the Company declines the Application, the Company will advise the reasons for its decision.

4.5 Repeat applications

If an application for approval via SRA of a Device is declined, the Company will only accept a repeat application and undertake the SRA Process again if the Device Approval Applicant can demonstrate a documented change in the security landscape or change in the Device justifying, in the Company's absolute discretion, reconsideration of one or more of the reasons for the Company's original decision.

4.6 Pilot Letter of Approval, Conditions for Pilot and Outcomes

4.6.1 *Pilot Letter*

(a) The Pilot Letter of Approval will:

(i) identify the security vulnerabilities disclosed in the SRA Assessment Report that are required to be mitigated before the technology could be accepted and published in the AusPayNet-Approved Devices List; and

(ii) detail the conditions of the Pilot in accordance with paragraph (b) below.

(b) The Pilot Letter of Approval will detail the conditions for the Pilot including:

(i) the liability shift to the Acquirer as set out in clause 4.6.3 below;

(ii) the restrictions of the Pilot which may include without limitation the General Conditions referenced in Table 2 below, customised as appropriate, by the Company in its absolute discretion; and

(iii) the Company's right to terminate the Pilot at any time during the Pilot by notice in writing to the Device Approval Applicant if, in the Company's absolute discretion, the Company determines the technology is vulnerable to a significant security threat or other security issue.

Table 2 Pilot - General Conditions.

General Conditions	Restrictions
Deployment Restriction	10- xx 000 instances/ deployments
Reporting	Fraud, Chargebacks, Merchant Category Codes
Functionality	Contactless only, no PIN
In flight Remediation	After **xx** Months **xx** vulnerabilities must be remediated
Term	3 to 12 Months
Future Approval	After **xx** months, Vendor must start certification against **xx** standard
Deployment	Vendor can only deploy in **xx** Merchant Category Codes
Liability Shift	Acquirer accepts liability for any fraud incurred during the pilot

4.6.2 *Outcomes*

(a) Following completion of a Pilot, or in response to a request from the Device Approval Applicant at any stage during a Pilot, if agreed to by the Company in its absolute discretion, the Company will:

(i) repeat the SRA to determine if the security vulnerabilities identified in the Pilot Letter of Approval have been mitigated; and

(ii) determine whether to:

(1) approve the Device;

(2) approve for Pilot as an extension of the current Pilot or as a Pilot under different conditions; or

(3) decline to approve the Non-Standard Technology in accordance with clause 4.4(d) above.

4.6.3 *Principles for Liability Shift during a Pilot*

(a) It is a principle applicable to any pilot that the Acquirer (being the Device Approval Applicant **or** the Pilot Sponsor) is responsible for card losses incurred by an Issuer, where:

(i) such losses arise from the compromise of PIN and/or card data;

(ii) the relevant compromise was caused by the use of a Device in a Pilot; and

(iii) the relevant compromise occurred during the term of the Pilot.

(b) Any claim must be raised either during the Pilot or during the period ending 2 years after the conclusion of the Pilot.

(c) The definition of losses will be limited to chargebacks and chargeback fees associated with fraudulent use of PIN and/or card data, and costs associated with re-issuing Cards.

(d) Upon an Acquirer identifying that the PIN and/or card data associated with the cards of two or more Issuers have been compromised at device under Pilot (or group of devices under Pilot), the Acquirer must immediately advise AusPayNet in writing.

4.7 Delta Applications

4.7.1 *Application for Approval*

(a) Where modifications are made to an Approved Device on the AusPayNet-Approved Devices List, a Device Approval Applicant may submit a Delta Application listing the modifications, following the process outlined in Part 4.3 above.

(b) The Company will undertake a Structured Risk Assessment of the Delta Application and determine whether the approval for the Approved Device should be updated to include all or some of the modifications listed in the Delta Application.

(c) The Company will notify the Device Approval Applicant in writing of its decision.

(d) If the Delta Application is approved, the Approval Period of the Approved Device will not change however the Company will:

(i) amend the AusPayNet-Approved Devices List noting the modifications; and

(ii) issue an updated Letter of Approval noting the modifications.

(e) If the Delta Application is declined, the Company will advise the reasons for its decision.

4.7.2 *Pilot Delta Approval*

(a) The Company may grant a pilot approval of the modified Device whilst the Delta Application under cl 4.7.1 is in progress, provided;

(i) The Delta Application includes a list of all changes made to the Approved Device; and

(ii) the Company considers the Delta Application and determines the risk of adverse impact on the security of the modified Device to be low.

(b) Where the Company approves a pilot under cl 4.7.2(a) above, the Company will issue a Pilot Letter of Approval to the Device Approval Applicant, detailed in cl 4.6, provided that the term of the pilot:

(i) will not exceed 12 months;

(ii) may be terminated by Company at any time during the Pilot by notice in writing to the Device Approval Applicant if, in the Company's absolute discretion, the Company determines the technology is vulnerable to a significant security threat or other security issue; and

(iii) will terminate automatically:

(A) on notification to the Device Approval Applicant of the Decision under clause 4.7.1 above; or

(B) on withdrawal by the Device Approval Applicant of the Delta Application.

PART 5 DISPUTE RESOLUTION

5.1 Reviewing a decision

(a) The Device Approval Applicant, Acquirer or any Third Party impacted by a decision made by the Company under this Device Approval Process may request a review of the decision.

(b) Any request for review must be made to the Company, in writing, within 30 days of publication of the decision or the Company's notification to the Device Approval Applicant, as appropriate. The request must identify:

(i) the decision and the date of publication or notification;

(ii) the reasons for the review;

(iii) the reasons provided by the Company for the decision that are disputed;

(iv) the grounds for disputing the decision; and

(v) all documentation or other material in support of the request to review.

5.2 Company response

(a) Within a reasonable period after receiving the request for review (reasonableness to depend upon the subject matter of the review request), the Company must review and advise its response in writing.

(b) The Company may request the parties meet to seek to resolve the dispute prior to issuing its response.

5.3 Appeal

(a) The party requesting the review may appeal the response by written notice to the Company within 10 days of receiving the written response.

(b) The appeal will be determined by an appeal adjudicator who will be nominated by the Company’s CEO.

(c) The party requesting the appeal must pay the costs of the appeal adjudicator and the reasonable costs of AusPayNet, unless the decision under review is varied.

(d) The Appeal Adjudicator may:

(i) confirm the Company’s decision; or

(ii) set aside the Company’s decision and substitute its own decision.

(e) The decision of the Appeal Adjudicator will be binding on the parties.

PART 6 GOVERNANCE

6.1 Review

The Company will review this Device Approval Process at least annually.