Australian Government

Department of Industry, Innovation and Science

STANDARD TERMS AND CONDITIONS

IN RELATION TO THE USE OF GOVERNMENT AUTHENTICATION SERVICES PROVIDED BY THE DEPARTMENT OF INDUSTRY, INNOVATION AND SCIENCE
(ABN 74 599 608 295) ('THE DEPARTMENT')

TABLE OF CONTENTS

PART 1. DEFINITIONS

1. TERMS

The following terms and meanings apply to these Standard Terms and Conditions.

Agency	An Agency that has entered into an MOU and an SLA with the Department for the provision of Government Authentication Services.
Agency Services	The meaning given in clause 2.
Agreed Maximum Transaction Threshold	The agreed maximum transaction threshold for a Service as set out in Schedule 1 of an executed SLA.
CA	Certificate Authority.
Commonwealth	The Commonwealth of Australia.
Confidential Information	All confidential, non-public or proprietary information of a Party (or of a third party to whom a Party owes an obligation of confidence) regardless of how the information is stored or delivered, exchanged between (or on behalf of) the Parties, relating to the business, technology, customers or other affairs of the Department, the Agency, or a third party, excluding information which: • is in or becomes part of the public domain other than through breach of this agreement or an obligation of confidence owed to the owner of the information • the disclosing Party can prove by contemporaneous written documentation was already known to it at the time of disclosure (unless that knowledge arose from disclosure of information in breach of an obligation of confidentiality) • the recipient acquires from another source entitled to disclose it.
Contact Officer	The contact person nominated by a Party for communication between Parties as detailed in an executed SLA.
CP	Certificate Policy.
CPS	Certification Practice Statement.
Credential	An electronic artefact that contains attributes about the holder of that credential. Attributes may assert the holder's identity, role or other authorisations.
Department	The Department of Industry, Innovation and Science.
Department PKI Terms and Conditions	Has the meaning given in the SLA.
Digital Certificate	A public electronic artefact that contains the user's public keys and is digitally signed by the PKI provider to ensure integrity.
Digital Credential	Has the meaning given in an executed SLA.
Disaster	An incident that results in a component failure within the infrastructure or applications used to deliver the Services.
EOA	Evidence of Authority.
EOI	Evidence of Identity.
FAS	Federated Authentication Service

Force Majeure	An event beyond the reasonable control of the Party affected.
Government Authentication Services	The authentication and timestamping services provided by the Department to the Agency, as listed in Schedule 1 of an executed SLA, and described in more detail in these Standard Terms and Conditions.
Intellectual Property Rights	All intellectual property rights, including but not limited to, the following rights: a. copyright and neighbouring rights, all rights in relation to inventions (including patent rights), plant varieties, registered and unregistered trademarks (including service marks), registered designs, Confidential Information (including trade secrets and know how), databases, and circuit layouts, and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields b. any application or right to apply for registration of any of the rights referred to in paragraph (a) c. all rights of a similar nature to any of the rights in paragraphs (a) and (b) which may subsist in Australia or elsewhere.
Internet Outage	The scenario whereby the internet service provider cannot source a connection to the internet.
ISM	The Australian Government Information Security Manual, or any replacement manual, in force from time to time.
Material	Documents, information, text and data stored by any means.
Material Change	A material adverse effect or a material adverse change on the operation of the Services as currently carried on by the relevant Party, or the imposition of a material liability on the relevant Party in any event or circumstance.
MOG Change	A Machinery of Government Change, being an allocation or reallocation of functions between departments and Ministers that materially impact the parties delivering the services under an agreement.
MOU	The Memorandum of Understanding which sets out the high level relationship between Parties.
Notification	A communication of an event anticipated by the Services which includes, but is not limited to, scheduled or urgent maintenance, unscheduled outage, and resolution of Service calls (each as described in the Standard Terms and Conditions).
Party	A party to a SLA.
PDS	PKI Disclosure Statement.
Personal Information	The meaning given in the Privacy Act.
Personnel	The Parties' officers, employees, agents, advisers, contractors and subcontractors (including their respective personnel).
PKI	Public Key Infrastructure.
Privacy Act	The *Privacy Act 1988* (Cth).
PSPF	The Commonwealth's Protective Security Policy Framework, or any replacement policy, in force from time to time.
Relying Party	An individual or organisation that acts in reliance on a Credential. The Services provide the Relying Party security tokens, which are assertions as to the validity of Credentials it authenticates.

Response Time	The time calculated from when a transaction is received by an application to when it is dispatched from the Department's internal processor. For clarity, the response does not include the internet or the Department gateway.
Scheduled Maintenance	As described in Attachment B.
Secondary Services	The secondary services provided by the Department to the Agency, as listed in Schedule 1 of an executed SLA, and described in more detail in these Standard Terms and Conditions.
Security Policy	The security policy developed by the Department in relation to the Government Authentication Services.
Services	Government Authentication Services and Secondary Services provided, or to be provided by the Department to the Agency as detailed in an executed SLA.
Service Performance Standards	The availability, latency and integrity standards set out in Attachment C.
SLA	The Service Level Agreement executed by an Agency and the Department.
Term	The period set out in an executed SLA.
Use	In relation to Material, includes to copy, reproduce, modify, make extracts from, display publicly or publicise, adapt, develop, integrate and (in the case of software) run, that Material or any adaptation of that Material.
User	An organisation, or individual person representing an organisation, that interacts or wishes to interact online with the Agency.
User Credential	A Credential, including a Digital Certificate, which has been issued to an organisation, or an individual person representing an organisation, for the purposes of interacting online with other organisations and which is supported by the Department as part of the Services.

1.1. Rules of Interpretation

In this Agreement unless the contrary intention appears:

a. (**reference to statutes**) a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them

b. (**law**) law means common law, principles of equity, and laws made by parliament (and laws made by parliament include State, Territory and Commonwealth laws and regulations and other instruments under them, and consolidations, amendments, re-enactments or replacements of any of them)

c. (**meaning not limited**) the words 'including', 'for example' or 'such as' when introducing an example, does not limit the meaning of the words to which the example relates to that example or examples of a similar kind;

d. words in the singular include the plural and vice versa

e. a reference to time is to Canberra time.

Headings are inserted for convenience and do not affect the interpretation of these Standard Terms and Conditions.

References to 'Attachments' are to an Attachment to these Standard Terms and Conditions.

PART 2. AGENCY OBLIGATIONS

2. SUPPORT FOR AGENCY USERS

2.1. Support services

a. The Agency acknowledges that it retains responsibility for delivery of Agency programs to its Users. The Agency will therefore be directly providing support services to its clients and will assist its Users to perform the relevant business activities (collectively, the Agency Services).

b. The Agency will provide 1st level support services for its Users for Agency business activities, including the provision of advice on how to interact with Digital Credentials and authentication services.

c. Where a User encounters difficulty or requires advice performing a business activity, the Agency will be the first point of contact for the User. The Agency's Help Desk support for their clients will then assist and advise the User as required, including in relation to compatible operating systems, system requirements, and computer set up.

d. The Agency will, on behalf of the User, escalate a problem it cannot resolve itself on the following basis:

   i. where the problem relates to the User's Credential, the User will be redirected to the issuer of that Credential

   ii. where the problem relates to the Services, the Agency will request technical support services from the Department.

e. The Agency is responsible for offering the User an alternative way to complete their business activity.

f. The Agency will not redirect a User to the Department Technical Support Desk Services under any circumstances.

g. The Agency will use the Department Technical Support Desk Services in accordance with clause 10.

2.2. Agency responsibility for Agency Services

a. The Agency must consider the following prior to commencing provision of any Agency Services:

   i. provision of Help Desk support for their clients

   ii. management of potential risks that may arise

   iii. business continuity should the internet, the Services or other services the Agency relies on not be available

iv. ensuring Digital Certificates and client records are kept secure.

b. The Agency and its Personnel must ensure the Services are not disrupted or misused, including informing the Department immediately of any potential disruption or misuse, and working with the Department to minimise the risk of such disruptions and misuse.

c. The Agency agrees that the Department has no responsibility or liability for managing the risk associated with the Agency Services.

2.3. Directions from the Department

The Agency will comply with any reasonable direction given by the Department (or a third party authorised by the Department) for the purpose of providing the Services, including:

a. the implementation of security updates

b. the alignment of the Agency's integration to the Services

c. ensuring the provision of effective Services.

3. MINIMUM REQUIREMENTS FOR AGENCY SYSTEMS

a. The Agency will notify its Users of the minimum platform requirements specified by the Department for each User Credential they will use.

b. The Agency acknowledges that these are minimum platform requirements and without these, the Department may be unable to provide the Services.

c. If the Agency becomes aware of any matter which:

i. adversely changes or could adversely change the scope, timing, performance levels or utilisation of the Services

ii. adversely affects or could adversely affect the Department's obligations and performance under this agreement

iii. adversely affects or could adversely affect the Service parameters for the operation of the Services

(each a Significant Event), the Agency must give written notice of the significant event to the Department within a reasonable timeframe prior to the significant event occurring, with particulars of the significant event.

d. If the Agency gives notice to the Department under this clause, the Department may, without limitation:

i. direct the Agency to take all reasonable steps to minimise the impact of the significant event upon the scope, timing, utilisation or performance generally of the Services or the Service parameters

ii. take any other reasonable action the Department considers in its absolute discretion in order to meet the Service Performance Standards

iii. alter the Service Performance Standards to reflect the impact of the significant event, either temporarily or permanently.

4. AGENCY OBLIGATIONS RELATING TO FAS

a. The Agency must ensure that the Agency's Identity Management System, and any other information that the Agency provides to the Department for the purposes of the Federated Authentication Service, is complete and accurate and does not cause an erroneous authentication by the Department through the Federated Authentication Service.

b. The Agency is responsible for any loss or liability suffered by, or any claim against, the Department as a result of an erroneous authentication through the Federated Authentication System that is caused by a breach of clause 6(a).

c. The Agency must:

i. ensure that the Agency's use of the Federated Authentication Service is permitted under, and is consistent with the terms of, the Agency's arrangements with other parties for the provision or receipt of the services in relation to which the Federated Authentication Service will be applied (**Service Arrangements**);

ii. use its best endeavours to ensure that the Federated Authentication Service is compatible with the services provided or received under any Service Arrangements; and

iii. ensure that any Service Arrangements provide that the other party to the Service Arrangement will not be responsible for any failure or delay in the conduct of those transactions resulting from interruptions to the Services that are not caused or contributed to by that party.

PART 3. THE DEPARTMENT'S OBLIGATIONS

5. SERVICES PROVISION

The Department will use its best endeavours to provide the Agency with the Services in accordance with the Service Performance Standards, as set out in Attachment C.

PART 4. OTHER PROVISIONS

6. CONSISTENT BRANDING

Both the Agency and the Department will use terminologies and a consistent brand in relation to the Services such that Users become familiar with and trust the role of the Department in the provision of the Services.

7. SECURITY

7.1. Notification and cooperation between Parties

a. To ensure the Services maintain a high level of integrity, each Party will notify the other Party if any of the following events occur:

   i. any security incident arising under this Agreement; or

   ii. any activities associated with remedying security incidents arising under this Agreement.

b. The Parties acknowledge that they may need to cooperate to mitigate emerging security vulnerabilities that may impact on the Services.

7.2. The Department Digital Credentials

a. The Department will require the Agency to sign transactions to the Department using Digital Credentials to ensure that it is the Agency requesting services from the Department and passing Agency User information to the Department. As part of the Services, the Department will issue Digital Credentials to the Agency to enable authentication of communications between the Agency and the Department in the form of service requests and responses.

b. The terms of use of the Department Digital Credentials are prescribed in these Standard Terms and Conditions and the Department PKI Terms and Conditions.

c. The Agency is responsible for the security of the Department Digital Credentials and associated keys provided by the Department.

d. In relation to the Department Digital Credentials and associated keys and information provided to the Agency, the Agency will:

   i. ensure that all information provided, and any representations made to the Department are up-to-date, complete and accurate

   ii. promptly notify the Department in the event that any part of that information changes

iii. accept sole responsibility for the contents of any transmission, message, or other document signed using the Department Digital Credentials and associated keys issued to the Agency by the Department

iv. perform any additional requirements as specified in the specific policy under which the Department Digital Credentials were issued, for example in the applicable VANguard Agency Certificate Policy (CP) or VANguard Agency PDS

v. only use the Digital Credentials and associated keys within the limits specified in the VANguard Agency CP and/or VANguard Agency PDS under which the Digital Credential was issued

vi. take all reasonable measures to protect their private key(s) from compromise and take all necessary precautions to prevent loss, disclosure, modification, or unauthorised use of their private key(s)

vii. only use the Department Digital Credentials and associated keys for the purposes authorised and not for any other purpose, including for any unlawful or improper purpose

viii. conduct their own independent risk assessment when using the Department Digital Credentials and associated keys for applications other than directly with the Services (if any such use is authorised)

ix. promptly notify the Department if they consider or suspect there has been a compromise of their private keys, and

x. promptly notify the Department if they consider the EOI or EOA information provided by them is, or may be, incorrect.

7.3. Agency's responsibilities when acting as Relying Party

When acting as a Relying Party, the Agency will:

a. verify that the VANguard Digital Credential is current and has not been revoked or suspended, in the manner specified in the VANguard CP/CPS/PDS under which the Digital Credential was issued

b. verify that the Digital Credential is being used within the limits specified in the VANguard CP/CPS/PDS under which the Digital Credential was issued

c. promptly notify the Department if there has been, or the Agency suspects there may have been, a compromise of their private keys.

8. RESTRICTIONS ON PUBLICITY

The Parties may not make media or other announcements relating to the provision of the Services without the prior consent of the other Party to the form, content and manner of the announcement or release, except to the extent that the announcement or release is required to be made by law or by a stock exchange.

9. TECHNICAL SUPPORT DESK SERVICES

Technical Support Desk Services are set out in Attachment A.

10. PRIVACY

10.1. Handling of Personal Information

a. The Department will securely store any Personal Information passed to it by the Agency in consuming the Services.

b. The Agency remains responsible for the User's Personal Information, and any correspondence in relation to that Personal Information should be addressed to the Agency.

c. The Agency acknowledges that the Department relies on the Agency's compliance to the Privacy Act and the Agency warrants that it will comply with the Privacy Act, including by obtaining all consents and providing all notifications required under the Privacy Act in relation to the disclosure of Personal Information by the Agency to the Department, and the collection, use and storage of that Personal Information by the Department for the purposes of performing the Services.

10.2. User Credential requirements

The Department will only accept User Credentials, which contain Personal Information, where the relevant Certificate Authority (CA) or Credential issuer has granted the Department permission for that Credential to be used by other agencies.

10.3. Disclosure of information

a. Subject to clause 10.3(b), the Department will not provide any information it receives from the Agency in providing Services to any organisation except the Agency, except where required by law to do so.

b. For agencies that choose to utilise the AUSkey credential, the Department will provide a copy of the Agency's AUSkey Transaction Report to the Australian Business Register (ABR).

10.4. Handling of User transactional information by the Department

a. The Department will maintain security controls around the information it stores in logs to ensure all access to the logs is recorded and that access is by authorised Personnel only.

b. The Department will ensure that the Agency is aware that sensitive User information should not be passed to the User Authentication Service.

c. The Department will have a record of every:

   i. Agency a User transacts with via Government Authentication Services; and
   ii. User the Agency transacts with via Government Authentication Services.

d. The Department will record the following information:

   i. the time and date of each transaction via the User Authentication Service;
   ii. the User IP address used via the User Authentication Service;
   iii. the name on the User Credential which may be the name of an individual (where provided) – except for the Federated Authentication Service;
   iv. the business information on the User Credential (where provided).

e. The Department will not save or store transaction content information relating to the transaction between the Agency and the User.

10.5. Access and Correction

a. The Department acknowledges that it has an obligation under the Privacy Act to give a User, who asks for it, access to any record of Personal Information about them held by the Department.

b. The Department will not change a historic record should that record be found to be inaccurate by either the User or the Agency. The Department will maintain all records in their original state for forensic and evidentiary purposes. The Agency will acknowledge the Department's role as an independent source of evidentiary information as it occurred through the Services, and that the Department is not the source of truth in regards to the information it receives in providing the Services.

10.6. Personnel and subcontractors

a. In relation to any Personal Information the Parties receive in connection with the SLA, each Party will:

   i. ensure Personnel requiring access to the information are under a legal obligation not to access, use, disclose or retain the information except in performing their duties of employment or engagement (as applicable)

   ii. notify the other Party promptly if a Party becomes aware of a breach of this clause by itself or by any of its Personnel.

b. Each Party will include restrictions on the use and disclosure of Personal Information in any subcontract entered into for the purposes of the Services that provide equivalent or greater protection to this clause.

11. INTELLECTUAL PROPERTY

11.1. Existing Department Material

The Agency acknowledges that the Department (and its service providers) owns the title to and the Intellectual Property Rights in or in relation to all Material relating to the Government Authentication Services, including:

a. policies and procedures

b. business descriptions

c. technical specifications.

11.2. Licence of the Department Material

The Department grants the Agency a non-exclusive, perpetual, irrevocable, world-wide, royalty-free licence (including the right to sublicense to the Agency's contractors) to Use any Material embodied in any of the Department Material, for the purpose of receiving the Services under the SLA.

12. IP INFRINGEMENT

Each Party is responsible for ensuring that its Material does not infringe the Intellectual Property Rights of any third party. Each Party will inform the other Party of the steps it is taking to ensure that no infringement occurs promptly on request from the other Party.

13. TERMINATION CLAUSE

13.1. Termination for convenience by Agency or the Department

Either Party may at any time, by giving 90 days' notice to the other Party, terminate the SLA in whole or in part.

13.2. MOG change and transition out

a. In the event that the Department is subject to externally imposed changes, such as MOG changes, that impact on the provision of Services, the Department will continue to provide the Services under the SLA until new arrangements are in place.

b. Where an event under clause 13.2 (a) occurs that changes the legal identity of the Department, the SLA will be terminated following transition to the new service provider.

c. On the expiry or termination of the SLA by the Department:

   i. the Agency will provide the Department with all reasonable assistance and information to assist in transitioning to the new service arrangements (if applicable)

   ii. the Department will promptly return all of the Agency's Material to the Agency Contact Officer, provided that the Department may keep a single copy for its records.

13.3. Compensation on termination

No compensation is payable by either Party on termination under this clause 15, in whole or in part.

14. NOTICES

A notice, approval, consent, instruction or other communication in connection with the SLA will be in writing and marked for the attention of the Contact Officer.

ATTACHMENT A - GOVERNMENT AUTHENTICATION SERVICES INFORMATION

A	**Services**	The Services available from the Department are: **1. User Authentication Service** The User Authentication Service provides real-time authentication of business users via the Department's authentication web page. The Agency redirects their business users to this web page at the time of login to be authenticated. This User Authentication Service enables the Agency to obtain an authentication token User's digital signature to facilitate business user access to an Agency secure web site or application. **2. Signature Verification Service** The Signature Verification Service eliminates the requirement for signed paper forms by providing verification of a business user's digital signature on signed electronic (XML) business forms. **3. Timestamping** Timestamping provides independent, verifiable evidence of the date and time of an electronic transaction. This Service utilises certificated time provided by the Department's National Measurement Institute. **4. Security Token Service** The Security Token Service facilitates secure transactions between business to government and government to government systems. This Service was developed to meet the authentication requirements of the Standard Business Reporting program. **5. Federated Authentication Service** The Federated Authentication Service allows agencies to provision and manage access to external applications for their own staff. It provides authentication for inter-agency systems whereby Users can use their credentials in their own agency to seamlessly access a service provided by a different agency. **6. Self Service Authorisation Portal** The Self Service Authorisation Portal is a website that allows AUSkey credential Administrators to authorise users within their organisation to perform tasks in participating AUSkey enabled websites.
B	**User Credentials Recognised by the Department**	The details of the User Credentials recognised by the Department can be found at www.vanguard.business.gov.au
C	**Secondary Services**	The Secondary Services available from the Department are: • certificate issuance Service (third party test and production environments) • third party test environment • reporting service (for Government Authentication Services and Technical Support Desk) • Technical Support Desk • external monitoring portal.

D	**Issue of Digital Credentials**	**Credential Issuance** The Department will provide the Agency with Digital Credentials for the purposes of authenticating Service requests for the Services. The Department will manage the following aspects of the Digital Credentials issued to the Agency: • notification of pending expiration of a Digital Credential • revocation of a Digital Credential upon request • re-issue on expiration or revocation of a Digital Credential. The Department will only revoke the Digital Credential issued to the Agency where the request for revocation originates from the Agency Contact Officer or the Agency Technical Support Desk. The Department will provide the Agency with a Digital Credential to access the production and third party test environments for the Services that the Agency has agreed to utilise. The Department issues different Digital Credentials for use in the third party test environment and the production environment. The Department will issue Digital Credentials in accordance with the VANguard CPS. The Department will undertake a 100 point EOI check on the Agency nominated custodians when issuing Digital Credentials used in the Production environment.
E	**Third Party Test Environment**	The Department will provide the Agency access to an exposed testing environment for the Services. This environment is termed the third party test environment. Subject to the availability, the Department will not restrict the Agency's access to the third party test environment.
F	**Reporting**	The Department will provide the Agency with the following reports that allow the Agency to monitor compliance with this Agreement: Transaction Report –Government Authentication Services This report lists the individual transactions of the Services. The report is limited to the Agency's use of the Services. The report will indicate the Service and Service version. The report covers a calendar month. This report is not used to monitor compliance with this Agreement. *Frequency:* Monthly. *Timing:* Ten (10) business days after the calendar month. Government Authentication Services Availability Report This report lists Service outages for the Services. The report is limited to the Agency's use of the Services listed in their SLA. The report will indicate the Service and Service version. This report provides details of scheduled and unscheduled outages. This report will detail the date and duration of the outage and the reason for the outage. This report is used to monitor compliance with Service availability under the SLA (Attachment C). Frequency: Monthly. *Timing:* Ten (10) business days after the calendar month The Agency may only request data that originated from the Agency.

		Supported Formats The Department will support the following reporting formats: For document reports: • Portable Document Format (pdf). For data reports: • Microsoft Excel spread sheets (xls) • Comma Separated Value (csv). Delivery Methods The Department will deliver reports via the following methods: • by email, subject to size, volume and sensitivity of data presented in the report. All reports will be delivered to the Agency Contact Officer.
G	**External Monitoring Portal**	The Department will provide a public portal that indicates the availability status of the Services in real-time. The Department does not warrant the availability of the external monitoring portal. In the event of a Service becoming unavailable, the Department will issue the Agency a Notification as soon as possible.
H	**Technical Support Desk**	The Department will provide a Technical Support Desk for the Services. The Department will provide a tiered support model with a priority for restoration of Services. The normal hours of operation for the Technical Support Desk are: Normal Hours: 08:00 to 18:00 Monday to Friday. Outside of the normal hours of operation, the Agency will be directed to an on-call staff member who will assist with any issues relating to the availability of Services. Any issues not relating to the availability of Services will be actioned during normal hours of operation for the Technical Support Desk. These issues include, but are not limited to: • change requests • issues relating to the Department Secondary Services • requests for information (i.e. queries) The Department will make available to the Agency documented procedures for consuming the Technical Support Desk Services. Refer to the document *Production Customer Support Guide*. Contact details for the Department Technical Support Desk are: Email: servicedesk@industry.gov.au Telephone: (02) 6213 7007 or 1800 000 384 (Option 5).

I	**Limit of Services**	**Services not provided** The following items are not included with the Services: • the provision of SSL certificates to the agency • the provision of security related education • the provision of risk assessments for the utilisation of the Services • 1st level support services to Users • an alternate service should a Service be unavailable. The agency is expected to develop business continuity plans that do not rely on the Department. **Fit for purpose** The Department does not warrant that the Services are fit for purpose for Agency transactions. The Agency is expected to determine suitability. The Department will use its best endeavours to provide all necessary information to assist the Agency to determine suitability. **Accuracy** In relation to the authentication of a User Credential, the Department does not warrant: • the accuracy of a User Credential • that a User Credential has not been compromised beyond checking the CA's latest Digital Certificate revocation information. The accuracy of the CA's latest Digital Certificate revocation information will be determined when validating a User Credential. The Department will indicate in the service response how long ago the CA's latest Digital Certificate revocation information expired as reported by that CA. In relation to the User Authentication Service, the Department will not check: • the accuracy of information passed by the Agency for display to the User. The Department will expect these to be accurate • the accuracy or operation of the links passed by the Agency for display to or use by the User. The Department expects these Agency resources to be accurate and operating correctly.
J	**Utilisation of Additional Services**	The Agency may utilise additional Government Authentication Services under the SLA, subject to satisfaction, in the opinion of both Parties, acting reasonably, of the following procedure: • the Agency notifies the Department of its intent to utilise additional services • the Agency provides an Agreed Maximum Transaction Threshold value for any additional services • the Department must approve the Agreed Maximum Transaction Threshold value for the additional services • the Agency will meet the minimum testing requirements for any additional service before that service is utilised in the Department production environment. Upon agreement of any additional service, the Service Performance Standards and service parameters for these additional services will be appended to the SLA.

K	**Security Management**	1. In addition to the obligations provided at clause 7 the Department will comply with the security requirements detailed in the Security Policy. 2. The Department will provide a copy of the Security Policy to the Agency Contact Officer upon written request to the Department Contact Officer. 3. The Department will ensure the Services under this Agreement are secured and managed at a minimum of PROTECTED level. This clause includes, but is not limited to: • information and data, in both electronic and physical formats • ICT equipment • ICT and general facilities • off-site storage of data • personnel. The Department will ensure ICT computer operations Personnel have a security clearance of HIGHLY PROTECTED or Negative Vetting 1 (NV1) level. The Department will ensure that all key Material and all EOI information (whether in electronic or hardcopy form) is stored securely in accordance with: • the requirements of the PSPF • the ISM • the Privacy Act. 4. The Department will publish a document known as the VANguard CPS. This will be a written statement of the practices employed by the Department PKI in issuing, managing, revoking, and renewing or re-keying Agency Digital Certificates. 5. The Agency Digital Certificate type is described in detail in the VANguard Agency CP, and in summary in the VANguard Agency PDS. These policy documents inform the Agency of the rules governing the use of the Digital Certificates. The Agency will inform themselves of the contents of these documents and may only use the Digital Certificates for the stipulated purposes and in the stipulated manner. 6. The Agency agrees that it is bound by the VANguard CPS, and the VANguard Agency CP and VANguard Agency PDS.

ATTACHMENT B - SCHEDULED MAINTENANCE

A	**Maintenance**	**Maintenance Categories** The Parties acknowledge that system maintenance mitigates risk of instability in a Service offering. The Department has categorised maintenance as the following: • scheduled Maintenance • urgent maintenance • unscheduled outage. **1. Scheduled Maintenance** Scheduled maintenance windows are set in advance for upgrades which include, but are not limited to infrastructure, hardware and/or software, Services, routine health checks and maintenance. The Department will notify the Agency at least three (3) months in advance. The allocated periods for scheduled maintenance includes the 2nd weekend in May and the 2nd weekend in December, each beginning on the Saturday at 24:00 until Monday 07:00. Scheduled maintenance for the Services will be subject to the normal Department change control process, and system changes will be fully tested in a pre-production environment prior to deployment to production. **2. Urgent Maintenance** Urgent maintenance is planned to incorporate maintenance actions on the system. This has been recommended as a recognisable risk and will be rectified with little or short notice. Clients will be notified as soon as the scenario has been assessed. Services will be unavailable for no more than four (4) hours. **3. Unscheduled Outage** An unscheduled outage is an unplanned event that results in a Service outage. Given that the Department will maintain an active/active ICT facilities configuration to provide continuous availability of the Services, it is unlikely that an unscheduled outage will occur. An unscheduled outage may occur when: • the Government Authentication Services require a critical update subject to vulnerabilities identified in supporting infrastructure • an Internet Outage occurs that impacts the active/active ICT facilities • a Force Majeure event occurs. Where possible, the Department will provide the Agency with immediate Notification should an unscheduled outage occur. In any event, the Department will provide the Agency with Notification of the unscheduled outage within the first hour of outage occurring. The method of delivering the Notification will be subject to the communications channels available.

		The Department will provide the Agency with update Notifications every two hours until the unscheduled outage is rectified. Where possible, the Department will provide in its Notifications advice as to the expected timeframes for the unscheduled outage to be rectified. Once the unscheduled outage is rectified, including any restoration of data, the Department will provide to the Agency a Notification that the unscheduled outage has been rectified and the relevant Services are available. The Department will make every effort to ensure that unscheduled outages will not exceed four (4) hours duration.
B	**Notification Details**	**Service Outages** The Department will notify the Agency in the following Service outage scenarios: • scheduled maintenance where that maintenance will result in a Service outage – this will occur three (3) months prior to the event • urgent maintenance where that maintenance will result in a Service outage – prior Notification where possible as soon as the scenario has been assessed • unscheduled outage - the urgency of the maintenance will be assessed and prior Notification will occur where possible • incidents that occur due to an error that may affect the working experience for the Agency. The Department will send Notifications relating to Service outages to the Agency Technical Service Desk.

ATTACHMENT C - SERVICE PERFORMANCE STANDARDS

A	**Service Performance**	**1. Availability** The Department will meet the following availability rates in providing the Services: • 99.5% for standard business hours (08:00 to 18:00, Mon to Fri) • 98.5% for non-business hours. The availability rate for the Services is subject to the following: • the availability rate relates to the Department production environment • the availability rate excludes Internet Outages. **2. Latency** The Department will return responses from Services within these latency targets: • User Authentication Service – within three seconds for 95% of requests. • Signature Verification Service – within three seconds for 95% of requests for a 1MB file, XML or PDF with a single signature. • Timestamping Service - within three seconds for 95% of requests for 200KB files; within seven seconds for 95% of requests for 3MB files. • Security Token Service – within three seconds for 95% of requests. • Federated Authentication Service - within three seconds for 95% of requests. • Self Service Authorisation - within three seconds for 95% of requests. The Response Time provided in these Standard Terms and Conditions relates to the time taken from receipt of a transaction, to process that transaction and issue a response within the Department production environment. The Response Time excludes the following: • the time between a User and the Agency • the time taken to reach the Department's gateway • the time taken for a transaction to pass through the Department's gateway • public internet response times. The latency target provided in these Standard Terms and Conditions are subject to the Agency not exceeding the Agreed Maximum Transaction Threshold value specified by the Agency. The Agency Agreed Maximum Transaction Threshold is detailed in an executed SLA. **3. Integrity** Any transactions submitted by the Agency, will be clearly distinguished as either processed successfully or in error via the standard service response. All transaction requests can be replicated and will reproduce the same outcome, guaranteeing transaction integrity.

B	**Change and Release Management**	**1. Changes to Services** The Department reserves the right to upgrade or change the Services in response to, but not limited to, the following scenarios: • new technology • improved security • feature enhancements. The Department may institute changes to the system and the Services from time to time that the Department considers are for the common benefit of multiple parties, or for other reasons the Department considers appropriate. Changes may include: • additional Services being added • components of the Services being removed; or deprecated • changes to existing Services (including associated service delivery systems). Where the Department upgrades or changes the Services, the Department will make every effort to minimise the impact on the Agency and other agencies utilising these Services. The Department will meet the following release schedule and change management service parameters in relation to the Services: • The Department will inform the Agency of the proposed schedule for release of any new software versions, new Services and configuration changes. • The Department will notify the Agency on any proposed changes to the functionality of the software version for the Services. The changes are limited to correcting security or privacy related issues. • The Department will allow the Agency four (4) weeks to test any changed functionality of the software version being utilised by the Agency. • Upon receiving notification from the Agency, under clause 3.c, of a significant event, the Department will postpone all non-essential Material Changes during the significant event unless subsequently and otherwise agreed with the Agency. **2. Submitting a Change Request** The Agency may submit a change request in relation to the Services through the Department's Technical Support Desk. There are two types of change requests, namely: • new requirement - where functionality is required that is not currently available as a Service • enhancement - where modification is required to existing functionality within a Service. **3. Change Assessment** The Department will perform an initial assessment of the change request before approving or denying a change request, and may determine that an impact analysis is needed to identify the effects of implementing the change. The Department may consider any of the following (but not limited to): • expected benefits of the change

		• components of the system affected by change • versions of the system affected by change • impact on all agencies consuming Services • resources needed to implement the change • length of time to implement the change • alternatives. The Department in providing a Whole of Government service will need to consider the merit of change requests in this context. **5. Service Deprecation** In the event that the Department upgrades a software version of any of the Services, the Department reserves the right to cease supporting the previous version of the Service after three (3) years. The previous version of the Service will be maintained for a period of no more than 18 months by which time it will be decommissioned. During this period the Agency must plan and implement changes to ensure its compatibility with the current version of the Service. **6. Right to Decide** For the avoidance of doubt, the Department is ultimately responsible for approving or denying changes to the Services. **7. Notifying with the Agency** The Department will notify the Agency at least 30 days prior to making Material Changes to the Services. The Department will work with the Agency to upgrade to newer versions of a Service as they become available. **8. Service Versioning** The Department will control the versions of all Services. Version numbers will be assigned to each Service to assist with the management of releases. Version numbers will indicate whether the version is a major or minor release. *Major Version Release*: A major version is defined as a significant change that has been made to a Service affecting the implementation of the former Service. These will be represented as a X.0 major version increment of the Service. It can also be referred to as containing a 'breaking change'. This process will be conducted in accordance with these Standard Terms and Conditions, and will also invoke the deprecation of the previous version as specified in these Terms and Conditions. *Minor Version Release*: A minor version is defined as a change that has been made to a Service which should not affect the implementation of the former Service. These will be represented as 0.X minor version increment of the Service. It can also be referred to as a 'non breaking change' version. This process will be conducted in accordance with these Standard Terms and Conditions and will also invoke the deprecation of the previous version as specified in these Standard Terms and Conditions.

C	**Supported User Platforms**	In relation to those Services that interact with User platforms: • the Department will use best endeavours to support commonly used User platforms (i.e. operating systems and browsers). • the Department will use best endeavours to support new versions of commonly used operating systems and browsers. This will occur as soon as practical.
D	**Data Backup and Archiving**	**1. Backup** The Department will maintain data backup plans and undertake backup activities to ensure: • transactional data generated by the Services can be restored as required in the event of a Disaster • transactional data generated by the Services and system configuration data is available for reporting, auditing and evidentiary purposes. The Department will undertake the following backup activities: • daily incremental backups • full backups on a weekly basis. The Department will maintain backup information at its active/active ICT facilities. **2. Archiving** The Department will move backup data to an alternate location to maintain system resources and support business continuity. This activity is known as archiving. The Department will archive data once it has reached its maturity age. The maturity age will be no less than three (3) months. The Department will archive data on a monthly basis.
E	**Business Continuity and Disaster Recovery**	**1. Department ICT Facilities** The Department will ensure that the ICT facilities that the Department uses to deliver the Services have built in redundancy and are maintained at a ready state to minimise unscheduled outages. The Department will provide an active/active ICT facilities configuration whereby under normal operating conditions: • transactions are distributed across the ICT facilities • transactions are replicated across the ICT facilities. The primary purpose of maintaining an active/active ICT facilities configuration is to enable the Department to continue to deliver the Services in the event of a Disaster within one ICT facility. **2. Disaster Recovery** The Department will maintain Disaster recovery plans for the Services and the ICT facilities that the Department uses to deliver the Services. The primary objective of the Disaster recovery process is to restore Service availability followed by restoration of historical data. The Disaster recovery plans will be used to rectify the Disaster and restore normal operations. The Department will immediately invoke the Disaster recovery plans in the event of a Disaster. A Disaster covers any component failure of the Services or any component failure within the ICT facilities that the Department uses to deliver the Services.

		The Department will endeavour to avoid unscheduled outages in the event of a Disaster through the invocation of its business continuity plans. In the event that data is to be restored from onsite storage, the Department will recover the data within a four (4) hour period. In the event that data is to be restored from offsite storage, the Department will recover the data within ten (10) business days. The Department will only notify the Agency of a Disaster event where an unscheduled outage occurs. **3. Business Continuity** The Department will maintain business continuity plans for the Services and the ICT facilities that the Department uses to deliver the Services. The primary objective of the business continuity process is to be able to continue to provide the Services in the event of a Disaster. The Department will immediately invoke the business continuity plans in the event of a Disaster. The active/active ICT facilities configuration provides automatic redirection of transactions to an active facility should a facility become unavailable. The Department will not be able to continue to provide the Services in the event of a Disaster that results in all ICT facilities that the Department uses to deliver the Services becoming unavailable. This event will result in an unscheduled outage.