CONTENTS

1. CONTEXT 3
   1.1. Background 3
   1.2. Purpose 3
   1.3. Scope and application 3
   1.4. Policy 3
   1.5. The ICT Services Catalogue 4

2. KEY PRINCIPLES 4

3. IDENTITY AND ACCESS MANAGEMENT 4
   3.1. Overview 4
   3.2. Drivers 5

4. REQUIREMENTS 5
   4.1. Federated & remote authentication identity management summary 5
   4.2. Requirements 5
   4.3. NSW Identity Hub 6
   4.4. Use Cases / Scenarios 6
   4.5. Elements of the standard 9

5. DOCUMENT CONTROL 13

APPENDIX A – Standards 14
   Developing standards 14
   Management and implementation 14

APPENDIX B – Sample Password Policy (NSW Identity Hub Password Policy) 15

APPENDIX C – Identity Hub Logical Architectures 16

APPENDIX D – As a service terms 17

APPENDIX E – References 18
1. **CONTEXT**

1.1. **Background**

This Federated and Remote Authentication Identity Management Standard is a technical standard developed through the NSW Government ICT Procurement and Technical Standards Working Group (PTS Working Group).

This standard defines minimum government requirements for federated and remote authentication identity management solutions.

1.2. **Purpose**

The purpose of this standard is to provide technical guidance to NSW Government agencies when implementing federated and remote identity management solutions internally and when they are procuring these services.

It details the issues that need to be considered so each agency can identify the available options that best suit their business requirements, helping agencies achieve value for money through cost savings and improved flexibility of service offerings, and ensuring they can take full advantage of the benefits of federated and remote identity management solutions.

1.3. **Scope and application**

This standard applies to all NSW Government departments, statutory bodies and shared service providers. It does not apply to state owned corporations, but is recommended for their adoption.

For the purposes of this standard, federated and remote authentication identity management describes all elements of a supplier’s federated and remote authentication identity management solution.

This standard does not exhaustively cover all agency specific considerations. Agencies may need to assess any specific requirements they have in addition to those detailed in this standard.

1.4. **Policy**

The *NSW Government ICT Strategy* sets out the Government’s plan to build capability across the NSW public sector to deliver better, more customer-focused services that are available anywhere, anytime, and derive better value from the Government’s annual investment in ICT.

Developing whole of NSW Government ICT technical standards is a key initiative of the *NSW Government ICT Strategy*, driven by the ICT Procurement and Technical Standards Working Group. These standards leverage principles defined in the *NSW Government ICT Strategy* and the *NSW Government Cloud Services Policy and Guidelines*, and they support the NSW ICT Services Catalogue. In procuring ICT services agencies should also have regard to the NSW Government ICT investment principles, set out in *NSW Government ICT Investment Policy and Guidelines*.

The standards set out service definitions as minimum requirements that vendors must meet to be able to offer their services through the NSW Service Catalogue. This helps achieve consistency across service offerings, emphasising a move to as a service sourcing strategies in line with the *NSW Government ICT Strategy*, and it signals government procurement priorities to industry.

This standard should be applied along with existing standards, policies and guidance that make up the NSW Information Management Framework, as set out in the *Information Management*:
A Common Approach, and including the NSW Digital Information Security Policy. In addition, solutions should assist agencies in their alignment with the NSW Government Enterprise Architecture Strategy.

NSW Government agencies must carefully consider their obligations to manage government data and information. Contract arrangements and business processes should address requirements for data security, privacy, access, storage, management, retention and disposal. ICT systems and services should support data exchange, portability and interoperability.

More information on the development of standards for the ICT Services Catalogue is at Appendix A – Standards.

1.5. The ICT Services Catalogue

The ICT Services Catalogue provides suppliers with a showcase for their products and services, and an opportunity to outline how their offerings meet or exceed standard government requirements.

The standards, together with supplier service offerings in the ICT Services Catalogue, help to reduce red tape and duplication of effort by allowing suppliers to submit service details once. The offerings are then available to all potential buyers, simplifying procurement processes for government agencies.

Implementing this category management approach is embedding common approaches, technologies and systems to maintain currency, improve interoperability and provide better value ICT investment across Government.

2. KEY PRINCIPLES

The following principles guide the development and implementation of this standard.

- **Facilitating as a service:** Federated and remote authentication systems should support agencies in moving to as a service sourcing models (see Appendix D – As a service terms).
- **Interoperability:** Meeting this standard should help agencies achieve application and hardware interoperability, ensuring that agency systems enable appropriate information sharing across devices and applications.
- **Leverage existing identity management solutions:** The NSW Identity Hub has been established by the Office of Finance and Services (OFS) and enables all NSW Government agencies to leverage whole of government scale when purchasing services from the Identity Hub through a unique licensing model.
- **Mobile and flexible:** The identity and access management (IAM) solution should support modern office work practices including flexible arrangements, activity based working and hot desking.
- **Vendor / operating environment agnostic:** The federated and remote authentication system should be vendor and operating system agnostic. Devices such as laptops, notebooks, thin-clients should be able to connect to and access the network. The solution must be fully compatible with widely used operating environments.

See Appendix C – Identity Hub Logical Architectures for a detailed representation of the NSW Identity Hub.

3. IDENTITY AND ACCESS MANAGEMENT

3.1. Overview

IAM, which is taken to include authentication, is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.
IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise.

Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives.

An IAM system provides functionality for identity life cycle management and resource access control. IAM includes policies, processes and workflows for onboarding, offboarding, identity modification, provisioning, authentication, authorization and entitlement enforcement.

3.2. Drivers

From a business perspective, there are three drivers for IAM that Gartner has consistently identified across enterprises:

- **Control**: The ability to give the right people the right access to the right systems and information at the right times for the right reasons to enable the right business outcomes.
- **Accountability**: The liability that users have to the enterprise for proper use of their entitlements and the liability that enterprises have to legal and regulatory bodies for compliance.
- **Transparency**: The visibility provided by analytics and auditing to confirm accountability, to demonstrate performance metrics and to deliver access assurance according to policies.

4. REQUIREMENTS

4.1. Federated & remote authentication identity management summary

This section provides a more detailed description of the IAM business and technical requirements for NSW Government. It provides a consistent approach for all NSW Government agencies regardless of their size.

4.2. Requirements

An IAM project is as much a business project as it is a technology project. As such it is important to go through a rigorous planning and strategy phase before choosing a vendor. Once you have chosen a vendor it is then equally important to put in place the resources to ensure that the project is a success, this includes making available test systems and internal business resources including defining the stakeholders who will make decisions. Gartner provides a structured approach for IAM Initiatives, set out below:

- **Strategise and plan**: Draft a charter to gain agreement on the vision and mandate behind the project, in alignment with business goals. Scope the project, and establish resources, budget and governance systems. Integrate the project with strategic IT and business plans.
- **Architect solution**: Define the architecture, technology and standards for the project. Model business requirements, and detail specifications for solution delivery. Recommend how to implement the project. Define process detail and performance metrics. Communicate the plan. Consider how to obtain attributes, whether they are stored locally or obtained from a federated attribute authority.
- **Select solution**: Set requirements, and issue RFPs. Analyse market intelligence. Evaluate vendor/service provider options. Choose technologies and vendors/service providers. Negotiate service-level agreements and contracts.
• **Operate and evolve**: Operate and manage the implementation. Revise in response to feedback, risks and changing business requirements. Measure performance. Monitor use and compliance. Develop skills, and define best practices for users. Refine governance processes.

### 4.3. NSW Identity Hub

The Identity Hub is a whole of government identity and access management platform established by the Office of Finance and Services. The Identity Hub is based on the Oracle technology stack with the core technology provided by Oracle Identity Manager (OIM) and Oracle Access Manager (OAM) and delivered as a SaaS platform from the GovDC data centres.

It is a foundational piece of infrastructure that has strong alignment with the goals stated in both the NSW Government ICT Strategy 2013 and the NSW 2021 plan. By implementing the Identity Hub for their IAM requirements agencies will be able to reduce implementation time, costs and risks whilst also leveraging a proven technology platform and whole of government scale to reduce costs.

As a tier-1 IAM platform, the Hub supports a better, more customer-focused service delivery whilst driving better value for NSW Government and enabling numerous strategic ICT programs across the sector. It delivers the capability to share applications, information and data across the whole of government, allowing all stakeholders to access real-time information and services from anywhere, anytime. These capabilities are delivered easily and securely through a single user identity (GEN) to deliver superior customer-focused services to citizens and businesses at a reduced cost to government. This single user identity is then the primary key for accessing every service provided through the Identity Hub.

The Identity Hub’s architecture is shown at Appendix C.

### 4.4. Use Cases / Scenarios

This section sets out the Use Cases / Scenarios for assessing an IAM solution. These Use Cases / Scenarios are based on the following scenarios:

<table>
<thead>
<tr>
<th>Agency (internal/office)</th>
<th>Authentication within the agency, where the user is connecting from a location physically within the agency across internal secured data networks.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency (remote/mobile)</td>
<td>Internal authentication, but when the user is connecting remotely to the agency’s network. Multi-factor authentication should be considered essential for this form of network connection. This should include considerations for Bring Your Own Device (BYOD) scenarios.</td>
</tr>
<tr>
<td>Agency to agency</td>
<td>Authentication and identity federation across two or more agencies, which could be in different jurisdictions. Multi-factor authentication should be considered. Single or same sign-on provisions a consideration. Multi-factor authentication should be considered desirable for this form of network connection.</td>
</tr>
<tr>
<td>Agency to business</td>
<td>Authentication and identity federation between an agency and a business, corporation, NGO or other organisation type. Additional details may be defined in the future. Multi-factor authentication should be considered desirable for this form of network connection.</td>
</tr>
<tr>
<td>Agency to citizen</td>
<td>Authentication between an agency and a citizen. Additional details may be defined in the future. Multi-factor authentication should be considered desirable for this form of network connection depending on the information/system access being obtained.</td>
</tr>
</tbody>
</table>
‘Use cases’ anticipated in agencies are listed in the requirements table below.

Required elements are indicated with ticks in the corresponding columns. Elements of the standard are set out in more detail in section 4.5.

<table>
<thead>
<tr>
<th>Use Case / Scenario</th>
<th>Lifecycle management</th>
<th>Identity federation</th>
<th>Self-service – access request &amp; password management</th>
<th>Role-based access control</th>
<th>Service and application accessibility</th>
<th>Legislation and regulation</th>
<th>Privacy and compliance</th>
<th>Built-in standards and specifications</th>
<th>Multiple integration options</th>
<th>Disaster recovery and business continuity</th>
<th>Testing</th>
<th>Auditing and investigation</th>
<th>Workflow engine integration</th>
<th>Multi-factor authentication</th>
<th>NSW Government Data Centre</th>
<th>Cloud compliant hosting facility</th>
<th>Service level management</th>
<th>Multi-service broker provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency (internal/office)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Agency (mobile/remote)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Agency to agency</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Agency to business</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Agency to citizen</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
4.5. **Elements of the standard**

**Lifecycle management**

This includes sub-elements such as user lifecycle management, automated provisioning/de-provisioning and just-in-time provisioning. The option of just-in-time provisioning allows for user accounts to be created or updated when a user logs in.

Granting and removal of IT access should be managed at a level appropriate to key business applications and services. The provisioning process should be able to differentiate between elevated privileged access under emergency situations and normal business as usual activities. Coupled with role-based access control (RBAC), the governance and approvals of provisioning and de-provisioning of access will be managed through the self-service portals where applicable, and depending on the circumstances approvals will be sought or waived.

Integration of provisioning and de-provisioning processes with either one central government-wide HR system (desired state) or multiple HR systems will be a mandatory requirement as the processes will be driven by employee movements.

The provisioning solution will need to be able to manage storage of employee identities and provide the capability to replicate the information efficiently across the agency’s network structures or in a manner of the agency’s choosing.

Authentication and authorisation services will also be required to service application information about employee credentials, entitlements and roles.

The provisioning solution should also be able to integrate with direct end infrastructure components such as Windows and UNIX servers, mainframe and database technologies (e.g. SQL, Oracle, and DB2) as well as cloud based software as a service and infrastructure as a service solutions.

IAM solutions must define the procedures and processes to off-board from the platform. These should include:

- Operability of the system during the transition
- Ownership of intellectual property

**Identity federation**

Federation as a capability allows organisations to establish pre-authenticated relationships where a user object (employee, citizen, business partner etc.) is able to access a service or services inside and/or outside of the boundaries of an agency. IAM solutions must be able to provide seamless authentication without having to manage end user identities in related environments. Ideally this should include either single sign-on or same sign-on capabilities.

**Self-service – access request and password management**

A self-service capability will allow a user, or someone on their behalf, to request IT access changes through the system.

Another element expected of IAM solutions will be the provision of users with the ability to reset their passwords without service desk intervention. It should allow for the application and modification of the password policy, and any solution must meet relevant Government password policy (see Appendix B – Sample Password Policy).
Role-based access control

This capability allows agencies to map and manage granular access requirements by creating roles (i.e. groups of entitlements and privileges across applications) and then managing allocation of those roles to appropriate users.

Service and application accessibility

IAM solutions are business critical applications so they need a high level of availability. This includes establishing a web presence accessible from varying environments and devices, including mobile and tablet, while maintaining the confidentiality and integrity of the service.

Any solution must meet operational excellence requirements and define a clear Service Level Agreement (SLA) for transparent monitoring and escalation to address any deficiencies.

IAM solutions must have a high degree of resilience, as they are used for business critical applications:

- They must provide a capability to cater for a defined minimum number of concurrent users.
- The system must perform to a defined set of response times as set in SLAs.
- Core IAM solutions must be available 24 hours per day for 7 days per week as it will be used for business critical applications.
- System performance must be able to be measured, monitored and reported.

System upgrades must be designed with a controlled path to ensure that an IAM system is continuously operable. An IAM operator will need to advise stakeholders of any planned outages e.g. maintenance, upgrades etc. This includes a defined notification period for planned outages and in the event of an unplanned outage, a process needs to be established for notification of system availability.

Legislation and regulation

All IAM solutions must comply with NSW Government policy, legislation and regulations supporting best practice, including but not limited to:

- Government Sector Employment Act 2013
- State Records Act 1998
- Government Information (Public Access) Act 2009 (“GIPAA”)
- Health Records and Information Privacy Act 2002 (“HRIPA”)
- Privacy and Personal Information Protection Act 1998 (“PPIPA”)
- NSW Government Financial Management Framework

See Appendix E – References for a full list of references.

Privacy and compliance

Any solution should comply with the Privacy and Personal Information Protection Act 1998, the Health Records and Information Privacy Act 2002 and the Government Information (Public Access) Act 2009, which help protect personal information from unauthorised use.

Built-in standards and specifications

Any solution should support all major IAM open standards and specifications including but not limited to SAML, oAuth, OpenID and WS-Federation. This will allow multiple options for federation and integration.

IAM platform must provide a secure environment to protect all sensitive data held within, as such, where relevant, any solution should be an ISO 27001 certified environment with the requisite documented management controls.
Multiple integration options
IAM platforms must support the integration options agencies require. These might be:
- direct integration of the IAM platform with agency provisioning targets
- integration to an existing IAM platform

Training, technical documentation and support
IAM solutions should include all user documentation and training guides as part of the solution. IAM solutions should also be responsible for developing initial and ongoing training programmes that meet the requirements of the variety of agency stakeholders e.g. end user training, train the trainer etc.

Further IAM solutions should provide all technical support documentation.
IAM solutions should provide support for the service provided to ensure availability and functionality of the service. A proposed support model will support the resolution of technical or usage issues. It would be expected that as a minimum solutions are capable of supporting at least two (‘N’ and ‘N-1’) versions of the solution.

Disaster recovery and business continuity
An IAM solution must propose disaster recovery and business continuity plans that support business functions in the event of a failure of the solution. These plans will also outline the disaster recover methodology, including processes and tasks to be followed to reinstate the solution for operational use.

Proposed plans should include multiple disaster recovery scenarios and the likely reinstatement outcome (timeframe). These plans must be regularly reassessed and retested. Procedures and processes for disaster recovery should be in place. In the event of disaster recovery the time taken from notification of recovery to restoration of full application or service functionality should be no more than that defined by the applicable SLA.

Services, applications and systems using federated authentication systems must fail-to-no-access in the event the federated service is either not available or is unable to adequately service requests.

Testing
IAM operators should assist and provide input to all testing activities including but not limited to: the development of test plans; system integration and regression testing; user acceptance testing; and pre-production testing.

Auditing and investigation
All elements of the IAM solution must provide the agencies, the Auditor General and/or any other statutory body with the authority to do so the ability to audit and/or conduct investigations.

Workflow engine integration
This could be a core element of some solutions, or it could be a bolt-on third party solution.

Multi-factor authentication
The IAM solution must support multi-factor authentication to enhance security.

NSW Government Data Centre
Depending on the service offering and agency requirements, it may be possible to ‘burst’ some elements of services to other location(s) subject to agreement with the commissioning agency.

Burst data centres must be deemed ‘compliant’. If the ‘burst’ data centre facilities change to a location that is deemed unacceptable either to NSW Government or to the agency, the agency may need to re-examine either the ‘burst’ service or the full service.
Cloud compliant hosting facility

All relevant cloud services for the solution are to be provisioned from a compliant hosting facility. Compliant hosting is defined as having the following attributes and/or capabilities:

- The location of the hosting facility must be identified either by name and/or location (city and country) in any response
- The hosting location cannot be changed without first informing the agency concerned
- The service provider undertakes, maintains and provides access to SSAE 16 Service Organization Control (SOC) Type II reports (or equivalent) for the services and facilities in scope for the engagement
- The hosting facility must comply with minimum Tier 3, as defined by the Uptime Institute, ANSI TIA-942, or an equivalent industry standard.
- The hosting facility must be certified against ISO 27001; compliance with the following international standards is desirable:
  - ISO 9001
  - ISO 27002
  - ISO 20000-1:2011
  - ISO 14001

Other desirable certifications may include, but are not limited to:

- PCI-DSS v3.0 or later
- Australian Signals Directorate
- ASIO-T4
- Uptime Institute
- CSA

Also consider contractual obligations relating to the service provider allowing security assessments and treatment of outcomes as agreed with the client.

If the hosting facilities changes to a location that is deemed unacceptable either to NSW Government or to the agency and/or loses attributes and/or capabilities identified above, the agency may need to consider termination of services.

Service level management

Agencies will retain ultimate responsibility for service level management in any solutions engagement, which would ordinarily be covered by a SLA. Agencies, service-brokers and solution providers need to agree all SLA reporting and other related activities as part of any transition-in process.

Multi-service broker provision

Any solution provider must work within the confines of a multi-service provider environment where either the agency or nominated provider will perform broker service provision. This will be defined as one provider being made accountable for the provision of all associated services, whether these are provided by the provider itself, or other third-party providers.
5. DOCUMENT CONTROL

Document history

Status: Final
Version: 1.0
Approved by: Procurement & Technical Standards Working Group
Approved on: 4 June 2015
Issued by: NSW Office of Finance & Services
Contact: ICT Services, Service Innovation and Strategy Division, Office of Finance and Services
Email: standards@finance.nsw.gov.au
Telephone: (02) 9372 7445

Review

This standard will be reviewed in 12 months. It may be reviewed earlier in response to post-implementation feedback from agencies.
APPENDIX A – Standards

Developing standards

Development of a standard begins with identifying the need for a new standard, which is followed by the development of the standard in consultation with the industry and experts groups, including the Australian Information Industry Association (AIIA).

The following diagram outlines the process.

The PTS Working Group is chaired by the Office of Finance and Services and includes senior representation from across the NSW Government clusters.

Agencies engage with the PTS Working Group concerning services for inclusion in the ICT Services Catalogue. This drives the development of technical standards, where none exist. The PTS Working Group has the leading role in reviewing and endorsing the technical standards developed in response to agencies’ requirements.

The PTS Working Group is supported by two sub groups responsible for the areas of Telecommunications and Services & Solutions. The sub-groups are responsible for initial development and review of standards relating to their areas of responsibility.

Management and implementation

There is scope to modify standards through the NSW ICT governance arrangements as necessary. Standards are designed to add value, augment and be complementary to, other guidance, and they are continually improved and updated.

This standard does not affect or override the responsibilities of an agency or any employee regarding the management and disposal of information, data, and assets. Standards in ICT procurement must also address business requirements for service delivery.

NSW Procurement facilitates the implementation of the standards by applying them to the goods and services made available through the ICT Services Catalogue. Standards will also be available on the ProcurePoint web site.
## APPENDIX B – Sample Password Policy (NSW Identity Hub Password Policy)

<table>
<thead>
<tr>
<th>Example attribute</th>
<th>Description</th>
<th>Minimum requirement</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>The number of passwords that must be remembered in order to avoid frequent reuse of passwords.</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Maximum password age</td>
<td>The period of time (in days) that a password can be used before the system requires the user to change it.</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>Minimum password age</td>
<td>The period of time (in days) that a password must be used before the user can change it.</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Minimum password length</td>
<td>The length of the shortest acceptable password.</td>
<td>8 characters</td>
<td></td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Technical enforcement of password complexity requirements.</td>
<td>Requires characters from 3 of the following categories:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• English uppercase characters (A-Z)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Base digits (0-9)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• English lowercase characters (a-z)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Special characters (for example, !, $, #)</td>
<td></td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords.</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Account lockout duration</td>
<td>How long a locked-out account will remain locked following failed login attempts?</td>
<td>30 minutes</td>
<td></td>
</tr>
<tr>
<td>Account lockout threshold</td>
<td>The number of failed login attempts prior to an account being automatically locked.</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Reset account lockout counter after</td>
<td>The number of minutes following a failed login attempt before the counter is reset to zero.</td>
<td>30</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX C – Identity Hub Logical Architectures
### APPENDIX D – As a service terms

This standard aligns with the definitions provided in the *NSW Government Cloud Services Policy and Guidelines*:

<table>
<thead>
<tr>
<th><strong>As a service (aaS)</strong></th>
<th>As a service – Refers to how the solution is provided. “As a service” usually refers to services that are delivered via the cloud rather than locally or on-site, although this is not always the case. As a service solution components are usually funded from an operating expenditure budget unlike capital intensive ICT infrastructure and equipment.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BPaaS</strong></td>
<td>Business process as a service – Delivery of business process outsourcing (BPO) services that are sourced from the cloud, accessed via internet technologies, usually automated, and constructed for multi-tenancy. BPaaS drives standardisation of business processes across NSW Government as normal commoditised activities move to best practice, e.g. payroll.</td>
</tr>
</tbody>
</table>
| **Cloud-based services** | On-demand delivery of ICT services over a network, commonly over the internet, from a shared pool of computing resources. “Cloud” usually refers to where the solution is provided. Key characteristics of cloud-based services are:  
  - On demand self-service  
  - Broad network access  
  - Resource pooling  
  - Rapid elasticity  
  - Measured service with unit based pricing |
| **Community cloud**     | Exclusively shared by a number of organisations with common objectives, and it may be on or off premises. An example may be the sharing of cloud infrastructure among a number of agencies of the same government. |
| **Hybrid cloud**        | A cloud deployment using at least two different cloud deployment models. An example is using resources from a public cloud for displaying non-sensitive data, which interacts with sensitive data stored or processed in a private cloud. |
| **IaaS**                | Infrastructure as a service – The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources. The consumer is able to deploy and run arbitrary software, which can include operating systems and applications. Computing power, networking and storage is provided. |
| **PaaS**                | Platform as a service – Where applications can be developed and executed. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. |
| **Private cloud**       | Provided solely for the use of one organisation and managed by that organisation or by a third party, provided at the organisation’s premises or off-site. |
| **Public cloud**        | The cloud infrastructure is shared via the internet with many other organisations and members of the public. |
| **SaaS**                | Software as a service – The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. Full application functionality is delivered. |
APPENDIX E – References
Agencies should have regard to the following statutes, NSW Government policies and standards:

- AS/NZS ISO 31000 Risk management – Principles and guidelines
- DFS C2013-8 Data Centre Reform Strategy
- Electronic Transactions Act 2000
- Government Information (Information Commissioner) Act 2009
- Government Information (Public Access) Act 2009
- Health Records and Information Privacy Act 2002
- M2012-15 Digital Information Security Policy
- NSW Government Cloud Services Policy and Guidelines
- NSW Government Enterprise Architecture Strategy
- NSW Government Open Data Policy
- NSW Government ICT Strategy NSW Government ICT Technical Standards – Mobility Standard
- NSW Government Digital Information Security Policy
- NSW Government Information Classification and Labelling Guidelines
- NSW Procurement: Small and Medium Enterprises Policy Framework
- Privacy and Personal Information Protection Act 1998
- Public Finance and Audit Act 1983
- Public Interest Disclosures Act 1994
- State Records Act 1998
- TPP 09-05 - Internal Audit and Risk Management Policy for the NSW Public Sector