Please address each of the minimum requirements and attach or include any supporting documentation.

Response Template version 20231115

NSW Health Minimum Requirements for Secure Access Environments

Email completed documents or questions to MOH-DataGovernance@health.nsw.gov.au

|  |  |
| --- | --- |
| **Organisation Name (SAE Owner):** |   |
| **Secure Access Environment Name:** |   |
| **Key Contacts** | ***Authorised Person:*** *(Has authority to provide responses on behalf of the Secure Access Environment and attest to their accuracy.)* | **Contact Person:***(If different from authorised person.)* |
| **- Full Name:** |   |   |
| **- Position (role title):** |   |   |
| **- Email Address:** |   |   |
| **- Phone Number:** |   |   |
| **Date of Response:** |   |   |
| ***Note: Do not respond to the requirements until you have read and understood the NSW Health Minimum Requirements for Secure Access Environments Document.*** |

**1. Curated gateway**

1. All data and file movements (ingress and egress) occur via a curated gateway
2. Curation is facilitated by approved users and processes
3. The gateway supports multiple curation models (Optional)
4. Gateway actions and approved files are immutably captured and logged
5. Curation occurs in a timely and transparent manner

*If the environment does not meet the curated gateway requirements, do not proceed.*

**2. Contained environment**

1. Data and files are contained within project workspaces for storage and analysis
2. Project and role-based access controls are implemented
3. Transparent platform architecture allowing the requirements to be verified
4. Cut, copy, and paste to or from the environment is prevented

**3. Secure environment**

1. Demonstrated adherence to a recognised information security and technology standard
2. Security audits, testing, updates, and backups occur regularly; backups must not contravene the requirements
3. Network access to and from the environment is prevented (except to provide required functionality)
4. Hosted in Australia (whether physical or cloud infrastructure)
5. Users are authenticated using best practices
6. Encryption at rest and in transit for all data and files, including uploads to the gateway

**4. Analytics enabled**

1. Economically sustainable and offers flexible resources
2. Performant environment that can support big data and complex analytics
3. Common tools, software and packages are provided as standard
4. Non-standard software can be deployed at the discretion of the SAE (Optional)

**5. Platform governance**

1. Roles, responsibilities, governance policies, service expectations and liabilities are clearly defined
2. Clear policies and efficient processes for user management
3. Data retention and disposal policies are enforced - differentiated for project, archive, and gateway / audit data
4. Training and support for users and custodians is available
5. Processes for NSW Health to respond to data breaches, conduct audits and curate outputs
6. Processes for SAE reporting on projects with NSW Health Data, including breaches
7. Data Custodians, their delegates or trusted platform administrators load data to the environment directly
8. Compliance with relevant legislation