

**Cyber Clearance Requirements**

The NDIA recognises that the requirements detailed in this document may include proprietary information about your organisation. The NDIA will consider the use of Non-Disclosure Agreements for the management of your proprietary information. Failure to provide sufficient evidence of compliance may impact your ability to access the NDIA API Gateway.

**Cyber Security Assessment Criteria**

| **No.** | **Requirement** | **Low/Medium** | **High Critical** | **Typical Evidence Required** |
| --- | --- | --- | --- | --- |
| **1** | **Self-Certification or Independent Certification**(Please refer to the API Risk Assessment Matrix to support your self-certification) | (Mandatory) Self-Certification against either:* iRAP
* ISO / IEC 27001: 2022[[1]](#footnote-2)
* SOC2
 | (Mandatory) Independent Certification against either:* iRAP or
* ISO / IEC 27001:2022
* SOC2
 | **Self-Certification** Completed documentation demonstrating your conformance with the requirements (full control suite) of one of the approved security standards.**Independent Certification**Copy of certificate and the Assessor Report upon completion of certification.**If seeking conditional approval for independent certification:**Letter of Engagement with a start date, completion date, scope of work and assessor details. |
| **2** | **Personnel Security** | (Mandatory) You need to demonstrate that appropriate processes and procedures are in place for hiring, managing, and terminating employees and contractors. | (Mandatory) You need to demonstrate that appropriate processes and procedures are in place for hiring, managing, and terminating employees and contractors. | * Internal policy document detailing how employees maintain confidentiality of enterprise information.
* Process descriptions detailing pre-employment screening and separation procedures.
* Sample contracts detailing conditions of employment.
* Written confirmation will be required to confirm that no contractors or non-employees have access to the source code.

If they do personnel security provisions will apply. |
| **3** | **Encryption in Transit****(6-8 week period to upgrade from TLS 1.0)** | (Mandatory) Encryption in transit is enforced using an approved cryptographic protocol (for example, TLS 1.3) and algorithm as per the Australian Government Information Security Manual. Specifically,* TLS should be supported, but not SSL (and variant) or TLS v1.1 (or earlier)
* TLS v1.3 should be supported, or a clear roadmap (incl. date) for when it will be supported
* Similarly certificate should disallow earlier/insecure variants.
 | (Mandatory) Encryption in transit is enforced using an approved cryptographic protocol (for example, TLS 1.3) and algorithm as per the Australian Government Information Security Manual. Specifically,* TLS should be supported, but not SSL (and variant) or TLS v1.1 (or earlier)
* TLS v1.3 should be supported, or a clear roadmap (incl. date) for when it will be supported
* Similarly certificate should disallow earlier/insecure variants.
 | Information (e.g. documentation or screenshots) regarding the following:* Identify the software stack and/or libraries used to achieve TLS
* SSL certificates
* Showing HTTPS protocol being enforced
* Call to API
* TLS handshake protocol being enforced.
 |
| **4** | **Encryption at Rest****(2 weeks currently being worked on)** | (Mandatory) Encryption at rest is mandatory for data repositories that hold or manage NDIS Participants related information. Encryption of data at rest is enforced using an approved algorithm (for example, AES-256) as per the Australian Government Information Security ManualExamples may include; full-disk, container, application or database level encryption techniques. | (Mandatory) Encryption at rest is mandatory for data repositories that hold or manage NDIS Participants related information. Encryption of data at rest is enforced using an approved algorithm (for example, AES-256) as per the Australian Government Information Security ManualExamples may include; full-disk, container, application or database level encryption techniques. | * Screenshot showing encryption enabled at the database or disk level with the type of encryption at rest being used
* When using ‘out of the box’ encryption a licensing agreement or screenshot showing ‘out of the box’ encryption at rest enabled
* If using the infrastructure of a cloud provider to encrypt data at rest, an invoice or contract agreement could be provided or screenshot from within the cloud environment showing encryption enabled.
 |
| **5** | **Encryption Key Management** | (Mandatory) Encryption key management (including public key infrastructure (PKI)) covering the following three categories:* Asymmetric/public key algorithms
* Hashing algorithms
* Symmetric algorithms.
 | (Mandatory) Encryption key management (including public key infrastructure (PKI)) covering the following three categories:* Asymmetric/public key algorithms
* Hashing algorithms
* Symmetric algorithms.
 | An internal policy or equivalent document which covers the scope of encryption key management. This document should include details relating to:* generation
* distribution
* storage
* access
* renewal
* revocation
* rotation
* archiving
* length and complexity of keys
* destruction of compromised keys
* recovery.
 |
| **6** | **Audit Logging** | (Mandatory) Appropriate audit logging functionality is implemented by your software product to enable traceability of user access and actions. | (Mandatory) Appropriate audit logging functionality is implemented by your software product to enable traceability of user access and actions. | * Sample of a dummy access and event audit log
* A data dictionary that describes the data attributes and maps against key audit log components
 |
| **7** | **Data Hosting** | (Mandatory) Data hosting on shore by default. Offshore hosting arrangements (including redundant systems) are managed by exception only. | (Mandatory) Data hosting on shore by default. Offshore hosting arrangements (including redundant systems) are managed by exception only. | **On-shore data hosting*** Provider name
* Provider location (physical address)
* Redundancy location (physical address)
* Whether the provider is ASD certified or assessed against another security standard

**Off-shore data hosting**If you are storing data off-shore you will need to contact the DPO in the first instance. Please note this includes metadata. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Requirement** | **Low/Medium** | **High Critical** | **Typical Evidence Required** |
| **8** | **Security Monitoring** | Optional | (Mandatory) Security monitoring is in place.For example:* Network/infrastructure layer
* Application layer
* Transaction (data) layer
 | **Network / Infrastructure layer – relevant combinations of the below:*** Screen shots (product page, the management console page)
* Product purchase/ownership doco (e.g. receipts, front page of a contract of product/support/service)
* Configuration files
* Photos of the product
* Photos of SOC/SIEM centre (using the products).

**Application layer – relevant combinations of the below:*** Screen shots of the function page in the application
* Reports from the backend system.

**Transaction (data) layer – relevant combinations of the below:*** Reports from the backend system
* Previous unusual cases.
 |

### **API Risk Assessment Matrix**

|  |  |  |
| --- | --- | --- |
|  |  | **Data Domain** |
|  |  | **Reference Data** | **Product Prices** | **Plan** | **Budget** | **Claim** | **Document Upload** | **Document Download** | **Service Bookings** | **Quotations** |
| **Type 1 - Registered Provider, Plan Managers (Already have a Production PRODA account)** | **2** | **1** | **3** | **3** | **3** | **3** | **4** | **3** | **2** |
| **Type 2 - Independent Software Vendors, Aggregation Service Providers** | **2** | **2** | **3** | **4** | **4** | **3** | **4**  | **4** | **3** |

### **Risk Rating**

|  |  |  |  |
| --- | --- | --- | --- |
| Low  | Medium  | High | Critical |
| 1. **Green**
 | 1. **Yellow**
 | **3 – Orange**  | **4 – Red**  |

1. NDIA will accept current ISO 27001:2013 certificates and reports. [↑](#footnote-ref-2)