# Records Management and Security Policy

| | | | |
|---|---|---|---|
| Policy number | P77 | Version | 6 |
| Approved by Board on | 15 August 2024 | Scheduled review date | Aug 2029 |

## 1. Policy statement

The National Institute of Organisation Dynamics Australia Ltd (NIODA)'s records are its corporate memory and as such are a vital asset for ongoing operations, providing valuable evidence of business activities and transactions.

NIODA recognises its regulatory requirements as an Institute of Higher Education. NIODA is committed to implementing best appropriate record keeping practices and systems to ensure the creation, maintenance and protection of accurate and reliable records. All practices concerning recordkeeping within NIODA are to be in accordance with this policy and its supporting procedures.

## 2. Scope

This policy applies to all staff, candidates and students at NIODA.

This policy applies to all aspects of NIODA's operations. This includes but is not limited to:

- all candidate, student and staff records
- all records created during business transactions
- all applications used to create records including forms, emails, database applications, bookkeeping system, internal platform and NIODA's website.

This policy provides the overarching framework for corporate recordkeeping policies, practices or procedures. It also covers the eventuality of record access to staff, candidates and students in the event that NIODA ceases to operate.

## 4. Policy context

NIODA's recordkeeping policies and practices are integrated with the organisation's broader information management regime (including business systems and knowledge management). NIODA's Leadership Team develops all record keeping strategies, and is responsible for the design, implementation and review of all recordkeeping practices.

## 5. Legislation and standards

NIODA acknowledges the following laws that relate to records and information:

- *Archives Act 1983*
- *Electronic Transactions Act (VIC) 2000*
- *Evidence Act (VIC) 2008*
- *Freedom of Information Act 1982*
- *Privacy and Data Protection Act 2014 (VIC)*
- *Privacy Act 1988*
- *Higher Education Support Act 2003*
- *Security of Critical Infrastructure Act 2018 (C'th)*

NIODA's recordkeeping systems capture and maintain records with appropriate evidential characteristics in accordance with its obligations under these pieces of legislation.

## 6. Recordkeeping systems

NIODA's recordkeeping systems are dedicated to the creation and maintenance of authentic, reliable and usable records for as long as they are required to effectively and efficiently support business functions and activities.

The recordkeeping systems manage the following processes:

- creation or capture of records within the recordkeeping system
- storage of records
- protection of record integrity and authenticity
- security of records
- access to records
- disaster recovery of electronic records and
- disposal of records - unless otherwise authorised, all record disposal within NIODA must be undertaken in compliance with the organisation's approved disposal guidelines.

## 7. Responsibilities

The Board of Governance is responsible for the authorisation and overseeing of the recordkeeping policy. The Chief Executive Officer (CEO), with support from the Leadership Team, must manage this policy.

The Leadership Team is responsible for overseeing the design, implementation, and maintenance of this recordkeeping policy, as well as monitoring compliance. A report of *Legislative Compliance* is submitted to the Board of Governance annually.

The Leadership Team is responsible for managing records and recordkeeping within NIODA consistent with the standards described in this policy.

The Leadership Team is also responsible for maintaining the technology for NIODA's recordkeeping systems; including responsibility for maintaining the integrity and authenticity of records and for supporting and monitoring staff recordkeeping practices as defined by this policy. Creation, and support for the creation of records by staff is a part of normal business practices.

All staff are responsible for the creation of accurate and reliable records as defined by this policy.

## 8. Records Security

Records generated by NIODA are stored electronically and backed up in two secure hard drives (currently locked home office computers), and a secure cloud-based data storage facility.

Access to all documents is through application in writing to the Administration Lead. The Administration Lead is authorised to respond to requests for candidate and student records of results. To obtain this information, students/candidates must submit electronic copies of two forms of photographic identification and meet via zoom (with camera on) to verify their identity.

Any decision to allow access to records must comply with the *Privacy Policy*.

NIODA's strategy for disaster recovery covers electronic and paper based records. All current records are stored electronically. As above, to mitigate risk in the case of theft or disaster:

- electronic records are secured by two-factor password protection
- cloud-based storage is secure two-factor password protected.

All users avoid access to materials that contain viruses, spyware, ransomware, trojan horses, and keystroke loggers that may create a cyber security breach. Cyber security breaches are reported under the *Notifiable Data Breaches Scheme* and the *Security of Critical Infrastructure Act 2018.*

## 9. Candidate and Student Files

Candidate and student information is stored in electronic format. Files created for each candidate/student include the following identifiers for retrieval purposes:

- given name
- family name
- candidate/student identification number
- date of birth

Academic candidate and student files contain all information pertinent to the candidate/student's enrolment, administration, academic progress, and completion (where relevant). Each academic candidate/student file contains the following evidence from the following candidate/student related activities (where applicable):

- enrolment documentation / information (including address, email, phone number, work role and organisation)
- FEE-HELP documentation
- student ID
- year commenced
- course code
- course name
- assessment record for the period of enrolment
- special consideration applications and approvals
- Credit Transfer and Recognition of Prior Learning applications and approvals
- appeal and grievances documentation
- course completion and graduation
- any other significant documentation related to the candidate/student life cycle.

## 10. Data Retention Considerations

When determining whether a record is to be retained, archived or disposed of, the following guidelines are followed:

- administrative value – do the records still support an ongoing function?
- legal value – will the records be needed in the event of future litigation? What are the legislative requirements? Most records should be retained for seven years. Academic records to be retained for twenty-five years.
- financial value – do the records relate to any current or on-going financial transaction? Most can be disposed of after seven years.
- historical value – does the record reflect significant historical patterns or policies that have shaped NIODA?

There are no paper based records. Electronic records are disposed of in the following manner:

- Google - deleted data is immediately removed from view and is then processed for complete deletion from Google's storage systems, across two months, including a potential 30-day recovery period. Each storage system has its own deletion protocol, which may involve multiple passes or delays. Additionally, encrypted backups may retain data for up to six months for disaster recovery.
- Jotform - deleted data is permanently purged from the system after 30 days.

**11. Recordkeeping Technology**

NIODA's policy is to use technology to support its record keeping systems. Upgrades and technology changes are considered annually as part of the business systems and risk reviews. NIODA favours a secure cloud based technology solution engineered for education providers because of ongoing access to technology expertise otherwise not feasible to maintain within NIODA's own capability. The following systems are cloud based:

- financial records (Xero) - the Administration Lead, the CEO, the accounts staff member and the auditor have login access to the NIODA Accounting system with capacity to manage and change records.
- email - access to management of the Google for Education email account is only available to the Administration Lead, the CEO and the IT support provider.
- document management
- candidate/student records
- NIODA website is hosted by VentraIP and managed by the IT support contractor.

The technology emphasis is on adequacy without over investment. Initial reliance is therefore on using the Google for Education file formats. Candidate and student records beyond financial records are in Google Sheets format.

**12. Grievances**

Grievances and complaints related to records management and security should be taken up as per the NIODA Grievance Policy. The Grievance Policy is published on the NIODA website www.nioda.org.au/policies

**13. Publication**

This policy is publicly available on NIODA's website at https://www.nioda.org.au/policies.

**14. Related Documents**

Privacy Policy

Grievance Policy

Archives Act 1983

Electronic Transactions Act (VIC) 2000

Evidence Act (VIC) 2008

Freedom of Information Act 1982

Privacy and Data Protection Act 2014 (VIC)

Privacy Act (1988)

Higher Education Support Act 2003

Australian Standard for Records Management (AS ISO 15489)

Security of Critical Infrastructure Act 2018