NIDA

1. POLICY STATUS AND DETAILS

Policy Number	Tech02-1
Approving Authority	Executive Team (ET)
Date Implemented	March 2024
Current Version	1.0
Date of Review	April 2027
Contact Officer	Head of Technology
Related Policies, Procedures and Documents	• Admission Policy and Procedure • Student Handbook • Course/Subject Guides • NIDA Student Charter • NIDA Code of Conduct • NIDA Password Policy • Appeals – Non-Academic Complaints and Appeals Policy • Non-Academic Complaints and Appeals eForm • Misconduct Policy • Academic Integrity and Plagiarism Policy

2. DEFINITIONS

Term	Definition
Accredited Course	A course that is recognised under the Australian Quality Framework (AQF) and is registered with one of the two main regulatory agencies, being TEQSA (Tertiary Education Quality Standards Authority) for Higher Education and ASQA (Australian Skills Quality Authority) for Vocational Programs.
Cyber security	the measures taken to: • protect information and communications technology, electronic systems, networks, devices and digital information from compromise or interruption; and • facilitate rapid and effective detection and response to any compromise or interruption.
cyber security control	any management, operational or technical measure (including safeguards or countermeasures) put in place for cyber security.

Cyber Security Event	When a NIDA Information Resource state indicates a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.
Cyber Security Incident	A cyber security event that has been assessed to have a potential adverse impact on the confidentiality, integrity, or availability of NIDA Information Resource.
Device	any hardware, software, cloud-based services, communication devices or network.
Digital Information	information that is in a digital or electronic form and is stored, processed, or transmitted within an Information Service or an Information Asset, including electronic scholarly materials.
Excessive Use	when a user or process has exceeded established limits placed on the NIDA Information Resource or is consuming an NIDA Information Resource to a level such that service to other users is degraded, or where the actions of the user could cause degradation if the user is permitted to continue the practice or activity.
Hacking Tools	tools that are designed to facilitate the identification and exploitation of software or system weaknesses for the purposes of unauthorised access.
Information	any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical,
Information Resource	any Information Service, Information Asset or Digital Information. Information Service means any business or information function using one or more Information Assets including but not limited to: (a) application systems (including software-as-a-service); and (b) Information infrastructure services such as operating systems, databases, voice and data telecommunications services, administrative tools, process automation tools, network services, media services, file and print services, and email services. Also known as ICT service, IT service, or system.
Intentionally Compromised Machine	A NIDA Information Asset or personal device that has been intentionally altered by the user or with the knowledge of the user, to introduce a security vulnerability or malicious code, or otherwise lacks a cyber security control.
NIDA Account	access to NIDA Information Resources provided to holders of a NIDA student ID or a NIDA email address.
NIDA Digital Information	Digital Information that is owned by NIDA or under the custody of NIDA.
NIDA Information Asset	any Information Asset that is owned, leased, operated, or managed by any NIDA
Personal Device	Any non-NIDA owned or provided device that is used by an individual to access, store, process or transmit NIDA data or NIDA Digital Information. This includes desktops and laptop computers, personal digital assistants, tablets, smartphones, mobile PIN pads, radio communication devices, USB keys or any form of portable storage device.
Prohibited Material	Illegal content, such as:

	(a) child exploitation material including child pornography or material that instructs, promotes or incites child abuse; (b) content that shows extreme sexual violence or materials that are overly violent; (c) materials that provoke the viewer into committing crimes and carrying out violent acts. This might be material that instructs, promotes or incites violent acts; (d) material that vilifies or instructs, promotes or incites discrimination; and (e) content that promotes terrorism or encourages terrorist acts.
Restricted Material	content that is not prohibited but: (a) is obscene or pornographic and permitted by law; or (b) is material that instructs or promotes gambling. This includes sexually explicit material, media, art, and/or products, or anything else containing adult content such as online groups or forums that are sexually explicit in nature, and sites that promote adult services.

3. SCOPE OF POLICY

This policy applies to

a. all technology resources used by, operated by, or provided on behalf of NIDA;
b. all information collected, created, stored, or processed by, or for, NIDA on device and network resources;
c. all individuals who utilise, or are involved in deploying and supporting, device and network resources provided by NIDA.

The Head of Technology is responsible for:

- ensuring the accessibility of this policy by students, and
- implementation of this policy

All staff are responsible for supporting this policy and following procedure if they are aware of student breaches.

Students are responsible for:

- Being aware of and following the policy and procedure.

4. PURPOSE

This policy outlines the appropriate usage of NIDA's Information Technology systems for NIDA's vocational and higher education programs.
This includes, but not limited to:

- Use of NIDA Hardware Devices
- Use of NIDA Owned/Licensed Software or SAS Solution
- Use of NIDA Wired/Wireless Network
- Information Sent or Received via NIDA Internet and Intranet
- NIDA Metadata captured during general usage of all Systems.

5. PRINCIPLES

Information Technology Resources are vital for NIDA's teaching and learning environment and the operations of the institution. NIDA is committed to maintaining a respectful, safe, reliable, and secure technology environment

that allows NIDA to meet its organisational objectives, legal requirements, and ethical responsibilities.

6. POLICY

6.1 Compliance

6.1.1 NIDA requires its Information and Technology Resources to be used legally, ethically and responsibly.

6.1.2 All users of NIDA Information and Technology Resources must comply with:

- applicable laws, including (but not limited to) copyright, intellectual property, breach of confidence, defamation, privacy, contempt of court, harassment and cyberstalking, vilification and anti-discrimination legislation, and workplace surveillance legislation.
- NIDA policies and procedures.

6.1.3 Users must not use NIDA Information and Technology Resources to:

i) harass, stalk, menace, defame, vilify, or discriminate against any other person. Refer to the *Anti-Discrimination, Bullying and Harassment Policy - Student*.

ii) collect, use, or disclose personal information except in accordance with the NIDA Privacy Policy.

iii) copy, download, store or transmit material which infringes infringe copyright, breach NIDA software license restrictions the intellectual property of any other party. Refer to the *Intellectual Property (IP) Policy*.

iv) transmit material in contravention of the Spam Act 2003 (Cth).

v) represent or create the impression of representing NIDA unless explicitly authorised to do so.

vi) represent another person or claim to represent another person unless explicitly authorised.

vii) otherwise cause loss or harm to NIDA's reputation.

viii) Distribute junk mail, chain mail or for-profit messaging.

ix) Distribute commercial emails on behalf of NIDA (including marketing and promotional emails), unless all intended recipients have consented or the message is required by law, NIDA is clearly identified and there is a clear means for the intended recipient to opt out of further commercial emails of the same kind;

6.2 Freedom of Expression

NIDA values and respects the values the diversity of cultures, ideologies and perspectives within its community and is respectful of freedom of expression. However, these privileges must be exercised responsibly, and NIDA manages any conduct, which breaches relevant policies, standards or legislation including the Student Charter, and the Student Code of Conduct, in accordance with the Misconduct Policy.

6.3 User Responsibilities

6.3.1 Users are accountable for all activities originating from their personal NIDA accounts, or other NIDA accounts that they use, as well as any NIDA Digital Information they store, process, or transmit using, or while connected to, a NIDA Information Resource.

6.3.2 Users must take all reasonable steps to protect NIDA Information Resources from physical or digital theft, damage, or unauthorised use.

6.3.3 To protect access to NIDA Information and Technology Resources, individuals must:

a. only use the accounts provided by the NIDA for their own individual use;

b. securely store passwords that provide access to NIDA systems or information;
c. keep personal and NIDA-provided systems, used to access NIDA systems or information, free from known vulnerabilities by maintaining operational and up-to-date antivirus and keeping up-to-date with vendor provided security updates;

6.4 Prohibitions

6.4.1 To protect access to NIDA Information and Technology Resources, individuals must not:

a. use another person's account or assist or permit the use of NIDA Information Resources by an unauthorised person
b. share NIDA-provided, self-selected passwords or other authentication factors with other individuals;

test, bypass or attempt to circumvent NIDAs Security Controls or Protection Mechanisms(including an operating system)

c. not introduce malicious software such as viruses, worms, ransomware or trojans into the NIDA environment; and

d. not attempt to gain unauthorised access to NIDA Information Resources through the use of Hacking Tools (including sniffing, scanning, password guessing or exploitation) or other digital technologies or devices when accessing, using or otherwise engaging with NIDA IT Resources.

e. not use NIDA Information Resources, or personal devices, to maliciously compromise the confidentiality, integrity, availability or privacy of NIDA Information Resources or NIDA Digital Information.

f. not use NIDA Information Resources to access, display, store, copy, process, transmit or provide prohibited material.

g. not use NIDA Information Resources to access, display, store, copy, process, transmit or provide restricted material except:

i. for teaching and learning purposes
ii. in accordance with the laws of the land and NIDA policies
iii. with the written approval of your Course Leader

h. not intentionally bypass identity or other cyber security controls for a malicious purpose.

k. not connect an intentionally compromised device to NIDA Information Resources

6.5 Reporting Breaches

- Any person noticing a potential or actual cyber security incident must report it as soon as possible to the NIDA IT team.
- The loss, theft or damage to NIDA Information and Technology Assets must be reported at the earliest opportunity to the NIDA IT team.

6.6 Ownership of NIDA Digital Information and Right to Monitor

- All NIDA Digital Information stored, processed, or transmitted using any NIDA Information Resource:
  a. may be recorded and monitored on an ongoing and continuous basis, in accordance with NIDA Cyber Security Protocols.
  b. may be subject to the Government Information (Public Access) Act 2009 (NSW).
  c. may be subject to the Privacy and Personal Information Protection Act 1998 (NSW).
  d. may be subject to the Health Records and Information Privacy Act 2002 (NSW).
  e. may be subject to the State Records Act 1998 (NSW).
  f. will remain in the custody and control of NIDA.
- NIDA Digital Information may be retained for as long as required in accordance with relevant statutes, regulations, or for archival purposes and business needs.

6.7 Privacy compliance and access to NIDA Information Resources

- NIDA is committed to balancing all users right to privacy with the legitimate protection and proper
- usage of NIDA Information Resources. NIDA will take reasonable precautions to protect the privacy of users, however, the use of NIDA Information Resources is not considered a private action or conduct.
- Users should be aware that personal use of NIDA Information Resources may result in NIDA holding personal information about the user or others which may then be accessed and used by NIDA to ensure compliance with this and other policies. This information will be managed in accordance with applicable privacy legislation and the NIDA Privacy Policy.
- NIDA must use personal information only for the purpose for which it was collected. To the extent that NIDA does collect personal information through scanning, monitoring, and accessing NIDA Information Resources including connected personal drives and devices:
  a. scanning and monitoring of personal drives and devices mapped to a NIDA Information Asset will not unreasonably intrude into the personal affairs of individual staff or students.
  b. any such information will only be used for assessing compliance with this policy, other NIDA policies or procedures, or legislation; or identifying and addressing security threats to NIDA Information Resources and will not be used for any other purpose.
  c. any inspection, access or examination of NIDA Information Resources must be in accordance with the NIDA Cyber Security Protocols.
- The following approvals are required for access by a person other than the owner or custodian, to NIDA storage services and storage devices such as mailboxes, Microsoft O365 services, hard drives, and file shares that may also contain personal information.

Circumstance	**Approver**
For legal proceedings or as required by law (e.g. to comply with a Notice to Produce or subpoena).	CEO or their nominee
Cyber security purposes.	Head of Technology or their nominee
NIDA reasonably suspects that an individual(s) is not complying with legislation or UNSW codes, policies or procedures.	Head of Technology, or their nominee, and the Director of People and Culture

A student is absent from study and access is required for legitimate business purposes (for example, work continuity) or occupational health and safety reasons (for example, where there are reasonable concerns about the individual's health and safety).	Director Learning and Innovation or their nominee.
When an identified approver has a conflict of interest	CEO and or any two members of the Executive who do not have a conflict of interest

6.8 NIDAs Terms of Use

- NIDA will implement reasonable precautions to protect the security of NIDA Information Resources, however, NIDA is not able to guarantee that NIDA Information Resources will always be available, secure, confidential, or free from any defects, including malicious software.
- NIDA accepts no responsibility for loss or damage (including consequential loss or damage or loss of data) arising from the use of NIDA Information Resources, or the maintenance and protection of NIDA Information Resources.
- NIDA may take any necessary action in accordance with the NIDA Cyber Security Standards, to mitigate any threat to NIDA Information Resources, with or without prior notice.
- NIDA at all times reserves the right to:
    a. limit or terminate the use of NIDA Information Resources, with or without notice.
    b. view, copy, disclose or delete NIDA Digital Information stored, processed, or transmitted using NIDA Information Resources.
    c. monitor or examine the security of any device connecting to NIDA Information Resources, to determine or address a cyber security threat to NIDA.
    d. monitor, access, examine, take custody of, and retain any NIDA Information Resource.
- Access to a NIDA Information Resource, or storage, processing and transmitting of NIDA Digital Information (including email) may be delayed or prevented in the event of misuse or suspected misuse, or in the event of a security event or suspected event.
- NIDA may at any time require a user to:
    a. acknowledge in writing that they will abide by this policy.
    b. complete relevant training in NIDA policies and procedures.

6.9 Misuse of IT Resources

In the event of misuse or suspected misuse of NIDA Information Resources NIDA may:

a. withdraw or restrict a user's access to NIDA Information Resources.
b. commence disciplinary action:

6.10 Appeals

Any appeal related to this policy is governed by the non-Academic Appeals and Complaints Policy and procedure.

7. CHANGE HISTORY

Date	Change Description	Reason for Change	Author	Version
August 2023	New title Updated template Expansion of definitions, terms, Scope, Purpose Basic Formatting	Policy review	Kylie Black, Ramana Kirubagaran	Draft
March 2024	Minor	Approved by ET	Executive Team	1.0

8. Consultation/Benchmarking

Benchmarked against policies and practice from a number of higher education providers and other sources.

Relevant policy documents from the following are gratefully acknowledged:

- Macquarie University
- University of New South Wales
- Sydney University

Consultation: Academic Heads of Courses, students.

Legislation and Regulatory Frameworks	Australian Qualifications Framework Higher Education Threshold Standards 2021 Privacy and Personal Information Protection Act 1998 Disability Discrimination Act 1992 Disability Standards for Education 2005 Standards for Registered Training Organisations (RTOs) 2015 ASQA General Directions Copyright Act 1968 (Cth) Corporations Act 2001 (Cth) Health Records and Information Privacy Act 2002 (NSW) Privacy and Personal Information Protection Act 1998 (NSW) Spam Act 2003 (Cth)