ACCEPTABLE USE POLICY (AUP)

[Accessible from https://help.nscc.sg/aup]

Version 3.0
18 November 2022

1. Preamble

1.1 The following policies are intended to ensure that NSCC users utilise the national high performance computing (HPC) resources in a responsible and appropriate manner. Users are reminded that unauthorised access to NSCC's computer systems and data or inappropriate use of the resources may constitute a serious criminal offence and a breach of the Computer Misuse Act (Cap 50A, 2007 Ed). Users will be required to cooperate with, and may be required to assist in reviews, investigations and any legal matters arising from their misuse of NSCC's resources.

1.2 This policy document will continue to be updated as and when the need arises. All users will be bound to policies in the latest version of this document. Users can refer to the up-to-date version of the NSCC AUP via the URL indicated above.

2. General Policy

2.1 NSCC's computing and network resources are to be used for work associated to, and within the bounds of their approved projects.

2.2 Users shall not engage in the inappropriate use of NSCC's resources that impinges the reputation of NSCC, its stakeholders, other users or the Singapore government. Incidents of inappropriate use may result in the immediate termination of accounts, escalation to the users' organisations, potential investigations or legal recourse. Examples of inappropriate use include, *but are not limited to*:

a) Activities which may be deemed as fraudulent, harassment, cause embarrassment, sexually explicit, obscene, intimidating, defamatory, or which incites religious or racial sensitivities.
b) Downloading, copying, or distributing copyrighted materials without prior permission from the owner.
c) Downloading or storing large files or utilising streaming media for personal use (e.g. music files, graphic files, internet radio, video streams, etc. which are not directly related to their approved projects).
d) Advertising, solicitation, or commercial activities for personal gain.
e) Cyber/Crypto-currency mining.

2.3 Project administrators, usually the project applicant and Project Investigator (PI), will be held responsible for the team members' full compliance to the AUP.

3. Computer Accounts and Passwords

3.1 Users must only access the resources via their personal approved NSCC account. Each person in a research group should apply for their own individual account.

3.2 Users must not share their personal account information or passwords with other parties. Users shall not deliberately divulge, or through negligence, allow any person access to their account. Users shall also not access or attempt to access another user's account. Users shall exercise appropriate care to safeguard their credentials and shall not publicise their account password or private keys.

3.3 Users shall not attempt to hack, crack, guess or capture another user's personal credentials including computer passwords, PINs, pass phrases or private keys. Users who come across such personal credentials should report such activity to NSCC immediately.

4. Cybersecurity

4.1 Users shall NOT engage in any of the following activities:

a) Access unauthorised data or applications.
b) Attempt to circumvent NSCC cybersecurity systems.
c) Access or attempt to access other users' data without their express consent.
d) Attempt to exploit or probe the system for security loopholes in the NSCC network or other organisations networks.
e) Attempt to attack or to degrade the performance of the NSCC network or that of other organisations.
f) Collude with other users to cause damage to the NSCC network or systems.

5. Software

5.1 Users shall not use or distribute any software that is contrary to prevailing licensing agreements.

5.2 Users shall comply with the laws of Singapore with regards to copyrights and intellectual properties.

5.3 Users shall not install illegally obtained software into NSCC's system.

6. Data

6.1 NSCC's resources are meant for scientific and technological research. Therefore, any uniquely identifiable information of a personal nature which may fall under the prevailing Singapore Personal Data Protection Act (PDPA) shall not be stored on NSCC's resources, or should be anonymised. NSCC shall not be liable in any way whatsoever if users choose to store such information on NSCC's resources. Users will be deemed responsible for their own data and may be liable for any breaches of personal data residing in their projects.

6.2 NSCC has set the default permission for all user files to be owner accessible only. Users shall be responsible for setting the proper file permissions and access control lists (ACLs) as deemed appropriate for their files and their work. NSCC shall not be liable for any permissions or ACLs which are wrongly configured.

6.3 Refer to Appendix 1 for the Data Management and Retention Policy on NSCC.

6.4 All users and project administrators must be fully aware of our data retention policies as detailed in Appendix 1 to ensure no loss of their data and compliance of their respective institution's or employer's research data management policy (RDMP), general Data Management Policy (DMP) and other relevant policies.

7. Use of Internet

7.1 While the internet is generally accessible from the NSCC facilities, such internet access is meant for purposes directly related to the use of NSCC's resources. Users shall refrain from using NSCC's resources for routine internet access like general web browsing, e-mails, etc. even though such activities may be a legitimate part of the user's normal course of work.

7.2 Users shall not engage in network activities that are not related to the proper use of NSCC resources. These activities include, but are not limited to, sending unauthorised mass emails, spam, electronic chain letters, unauthorised participation in online chat groups, or engaging in denial of service (DoS) attacks.

7.3 Users shall not communicate material that can be deemed as fraudulent, harassment, cause embarrassment, sexually explicit, obscene, intimidating, defamatory, or which incites religious or racial sensitivities. Users shall not knowingly download such material from the Internet.

8. Prohibited Use

8.1 Nationals of countries under the Office of Foreign Assets Control (OFAC) Sanctions Programs to take note of any prohibited use.

8.2 Individuals from organisations on the US Control Policy Unverified List (Supplement No. 6 to Part 744) or who are themselves on the list are prohibited from using any of NSCC's resources. Such individuals with a legitimate need to use NSCC's resources may furnish a request to NSCC whose approval has to be explicitly granted before any such use.

9. Communications

9.1 As part of its ongoing operations, NSCC may send out advisory notices or announcements to users regarding the state of the system and new services/initiatives via email. By using

the NSCC system, users therefore grant NSCC the explicit consent, in accordance with the prevailing Singapore Personal Data Protection Act (PDPA), to send such emails. Users should take note of such emails (e.g., announcements on system status, maintenance schedules, etc.) and not to treat them as unsolicited spam or junk mail.

10. Citation and Presentation

10.1 All academic journal or conference papers or reports that have leveraged NSCC's resources shall acknowledge and cite NSCC with the following:

"The computational work for this article was (fully/partially) performed on resources of the National Supercomputing Centre (NSCC), Singapore (https://www.nscc.sg)."

10.2 All successful projects with such publications must report them to NSCC through the project deliverables update or otherwise.

10.3 Selected users may also be required to partner with NSCC to present a talk, article, paper or poster for NSCC's organised events (e.g., Supercomputing Asia conference, use case studies or other occasions where NSCC has a presence.