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

Version 2.1
8 February 2021

1. Preamble

1.1 The following policies are intended to ensure that NSCC users utilise the national high performance computing (HPC) resources in an 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 any legal investigations 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 uses will be bound to policies in the latest version of this document. Users can check for the up-to-date version using the URL stated above.

2. General Policy

2.1 NSCC 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. Incidents of inappropriate use may result in the immediate termination of accounts, potential investigations or legal recourse. Examples of inappropriate use include, but are not limited to:
   a) Activities which may be fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or which incites religious or racial intolerance.
   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.

3. Computer Accounts and Passwords

3.1 Users may access the resources only via their personal account. Users may not share their personal account information or passwords and have their own individual accounts, i.e. each person in a research group should apply for their own individual account.

3.2 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 person's personal credentials including computer passwords, PINs, passphrases or private keys. Users who come across such personal credentials should inform NSCC immediately.

4. Cybersecurity

4.1 Users shall NOT engage in any of the following activities:
a) Accessing unauthorised data or applications.
b) Attempting to circumvent security systems.
c) Accessing or attempting to access other users' data without their express consent.
d) Attempting to exploit or probe for security loopholes in the NSCC network or other organisation networks.
e) Attempting to attack or to degrade the performance of the NSCC network or that of other organisations.
f) Colluding with other users to cause damage to the NSCC network or systems.

5. Software

5.1 Users shall not use or distribute software 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 personally identifiable information which may fall under the Personal Data Protection Act 2012 (PDPA) shall not be stored on NSCC's resources. NSCC shall not be liable in any way whatsoever if users choose to store any such information on NSCC's resources.

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.

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 not use 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, 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 is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or which incites religious or racial intolerance. Users shall not knowingly download such material from the Internet.

8. Prohibited Use

8.1 NSCC's resources may not be used for the following purposes:

a) Development, production, use or stockpile of Weapons of Mass Destruction, including but not limited to nuclear weapons, chemical and biological weapons, rocket systems and/or unmanned air vehicles capable of a range of at least 300 kilometres or WMD-Related End-Use (*) as defined below.

b) Development, production, use of arms, including but not limited to military vehicles or military aircraft and accessories/parts thereof.

c) Other military applications.

> *(*) "WMD-Related End Use" means*
> *(i) production, development, usage or stockpiling of nuclear fuel/materials, research on nuclear fusion, nuclear reactors or parts/accessories thereof, production of heavy water, processing/reprocessing of nuclear fuel/materials; and*
> *(ii) development or manufacturing of chemical materials, production, development, usage or stockpile of microorganisms/toxins, production, development, usage or stockpiling of rockets/unmanned aircraft, research on space (astronomy excluded) by or on behalf of any military or other defence organisation.*

8.2 Nationals of the following countries are prohibited from using any of NSCC's resources: Iran, Afghanistan, Central African Republic, Democratic Republic of Congo, Ivory Coast, Eritrea, Iraq, Lebanon, Liberia, Libya, North Korea, Somalia, Sudan, Cuba and Syria. Citizens of these countries 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.

8.3 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 Personal Data Protection Act 2012 (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 shall 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 Select users may also be required to present a paper or poster in NSCC's Supercomputing Asia conference series or other internationally recognised supercomputing conferences where NSCC has a presence, typically in the form of an exhibition booth.