I NCL'S USAGE POLICY

A. Introduction

A.1. NCL provides the following services:

(1) Leasing of bare-metal servers
(2) Leasing of Virtual Machines
(3) Customised auto-provisioning of host & network using DeterLab
(4) Customised auto-provisioning of host & network using OpenStack
(5) Auto-provisioning of CVE environment via NCL CVE Catalog
(6) Auto-provisioning of NCL Secure Distributed Environment
(7) Auto-provisioning of NCL Hybrid Cloud Environment

(Hereinafter referred to as the "Services")

A.2. The specifications of the Services are described in Annexes (1) to (7).

A.3. The charges and payment modes for each of the Services are described in the Order Form.

A.4. This Usage Policy shall govern the use of Services (1) to (7). Use of the Services shall also be subject to directives from NUS and/or its School of Computing ("SoC") directives concerning usage of its IT facilities.

B. Eligibility Criteria for Users

B.1.1 A user shall create a new project (see Section B.2) or join an existing project to use the testbed's resources (see Section B.3).

B.1.2 Users wishing to undertake new projects meeting the requirements set out in Section 2 below shall be given priority.

B.2. Project Creation

B.2.1 A user shall apply for a new project with SoC's NCL.

B.2.2 The application will be reviewed and approved by NCL if the project meets the following requirements:

(1) It is a project from:

(a) Local Research Institution (RI), Academic University (AU), Institute of Higher Learning (IHL), as registered under the Ministry of Education of Singapore; OR

(b) Singapore government agencies, which can be found in the Singapore Government Directory (https://www.gov.sg/sgdi/ministries); OR

(c) Companies that are based in Singapore and registered under Accounting and Corporate Regulatory Authority (ACRA).

(2) The project performs the following activities:

(a) For the local RI, AU, IHL and government agencies:

(1) Research and Development

(2) Testing,

(3) Experimentation,

(4) Cyber Range/Exercises,

(5) Teaching/training.

(b) For companies, R&D projects that are in line with the themes of the National Cybersecurity R&D Programme of the National Research Foundation (see http://www.nrf.gov.sg/about-nrf/programmes/national-cybersecurity-r-d-programme).
Activities for the sole purpose of supporting a company's day-to-day operations such as the serving and hosting of data are inadmissible.

(3) The user applying for the project is eligible to be a project leader. In general, a user needs to be a Faculty member, or the equivalent R&D, teaching and management staff in the organisation to be eligible. Other staff from an organisation may apply to create a project if he/she is able to provide NCL written assurance that he/she meets the requirements. His/her application will be dealt with on a case-by-case basis.

NCL will perform verification of the application and reserves the discretion to reject the application.

B.3. Joining an Existing Project

B.3.1. A project leader may invite other users to join a project as project members. A user may join the project by accepting the invitation. A user may also browse projects which publish their information publicly in NCL and apply to join a project. He may join the project if the project leader accepts the application. The project leader shall verify the identity of the team members and ensure that they will honour the agreement he has signed with NCL. NCL reserves the rights to perform further verifications as and when needed.

C. Using NCL

C.1.1 A project team could make use of the resources of NCL to run experiment/conduct classes. Besides the above Services, a project leader or member may also bring in his own resources. The project leader shall ensure and declare that that the project team shall have obtained and/or shall obtain all necessary licences, and shall comply with all applicable usage conditions when using their resources in the testbed. For uncommon software/huge dataset that cannot be easily run in the nodes, or for hardware that requires integration with the testbed, NCL will reasonably endeavour to review requests to facilitate such usage and shall be entitled to subject such use to additional conditions and charges.

C.1.2 If an experiment or class requires Internet access, the project leader conducting the experiment or class shall seek permission from NCL prior to its commencement. This is to keep NCL appraised of potential risks and issues.

C.1.3 NCL will provide protection mechanisms to prevent one experiment from affecting another experiment. The project leader shall ensure that the

experiments will not affect other experiments, either by intentionally breaching the protection mechanisms or by other means.

D. Reservations and Prioritisation

D.1 There are two subscription modes to use the NCL resources:

Advance Booking of Thirty (30) days or more: For reservation received more than thirty (30) days prior to the commencement date of the requested usage period, such requests will be sent to Committee on the **third work day** of each calendar month. Users will be informed on the **fifth work day** of each month on the status of their Advance Booking reservation requests.

Short Notice Booking: For reservation received less than thirty (30) of the requested usage period, the reservation will be processed within 3 working days. Users may also use the resources on an ad-hoc basis without any reservation or booking, subject to **availability**.

D.2 Advance Booking

D.2.1 Users may make reservation of the Services through the Order Form. The Order From will state the start and end dates, the duration of usage, the number of machines required, and the number of users involved. The Order Form will also allow users to state alternative dates and time to improve the chances of having a successful reservation.

D.2.2 Pre-allocation checks will be done on the first and second work day of each month. The checks will:

(1) Review all the reservation cancellations made by the end of the previous month and take stock of the resource availability.

(2) Prioritise all the reservations made by the end of the previous month.

(3) Identify possible conflicts and attempt with reasonable effort to resolve the conflicts. Conflict resolutions include trying to contact the users to determine alternative dates and time for reservation.

D.3 Resource Allocation Meetings

Resource Allocation Meetings will be called on the third work day of each month. The meeting will:

(1) Confirm all the reservation cancellations made by the end of the previous month.

(2) Prioritize all the reservations made by the end of the previous month.

(3) Confirm all the reservations made by the end of the previous month.

D.4 Notifications

The user will be informed on the fifth work day of each month on the status of the reservations. The resource booking will also be updated on the website.

D.5 Prioritisation Order

D.5.1 The prioritisation will be done according to the following order:

1. Cyber exercises by government agencies
2. Cyber security research/demo/validation by AU, RI and IHL
3. Cyber security research/demo/validation by government agencies
4. Cyber security research/demo/validation by companies receiving government funding
5. Cyber security research/demo/validation by start-ups and SMEs
6. Cyber security research/demo/validation by other companies
7. Lessons by AU, RI and IHL
8. All other research/demo/validation by AU, RI and IHL
9. All other research/demo/validation by government agencies

D.5.2 NCL will review its prioritisation scheme on a regular basis (every 6 months) and reserves the right to amend the prioritisation system.

D.6 First Day of Reservation

Reservations of resources for cyber exercises by the government agencies and lessons by AU, RI and IHL can be made no earlier than twelve (12) months in advance. Reservations for all other activities can be made no earlier than six (6) months in advance.

D.7 Last Day of Reservation

Reservation should also be made at least one month in advance. This is to give some of the users running existing experiments sufficient time to conclude their work. Further, as the Resource Allocation Meeting is held monthly on the third work day of each month, and the resource allocation confirmed on the fifth work day,

(1) Order Forms received within the first five work days of a calendar month, shall not be processed until the next Resource Allocation Meeting held on the next calendar month .

D.8 Cancellation of Advance Booking

Cancellation of reservations may be made one month prior to the reservation date. Users will also be charged for cancellation made less than ninety (90) days prior to the commencement of the requested usage period as follows:

(1) For cancellation of the reservation received by SoC at least ninety (90) days or more prior to the commencement date of the requested usage period, no charges will be incurred.

(2) For cancellation of the reservation received by SoC at least sixty (60) days but less than ninety (90) days prior to the commencement date of the requested usage period– 30% of the charges (based on the charges for the requested usage period) will be incurred.

(3) For cancellation of the reservation received by SoC at least thirty (30) days but less than sixty (60) days prior to the commencement date of the requested usage period – 60% of the charges (based on the charges for the requested usage period) will be incurred.

(4) Less than thirty(30) days prior to the commencement date of the requested usage period – full charge will be incurred and shall be payable by the user.

Partial cancellations may be permitted subject to review on a case by case basis.

Short Notice Booking

D.9 Users may make short notice bookings of the resources less than one month in advance, or use the resources on an ad-hoc basis without any reservation or booking. These bookings/usages will be processed in a first-come-first-serve basis. Cancellation is not allowed and the user will be charged the full amount. Further, if a short notice booking, or an experiment from such booking, is in conflict with a reservation, NCL may request users to terminate the short notice booking or experiment. Users will be given the full refund of the unused resources.

E. Maintenance

E.1. Scheduled Maintenance

E.1.1 NCL will conduct regular maintenance to provide the best possible Services. During maintenance, NCL might need to reboot the system and some user activities might be affected.

E.2 Maintenance Schedule. The scheduled downtimes for regular maintenance are: First Sunday of every month, 7am – 7pm or otherwise scheduled. For Emergency Maintenance, NCL will make the best effort to notify users. Users will be reminded to back up their data on NCL Lab Environment to avoid any data loss or disruption during Maintenance (Neither NUS, SoC nor NCL shall have any liability for any loss of data or disruption). NCL will also publish all Maintenance information on website.

F. Intellectual Property (IP), Ownership & Usage

F.1 NCL will not own the IP created by the users in using NCL. In particular, NCL does not own the IP of the following (including their implementations):

(1) Algorithms

(2) Protocols

The IP ownership of artifacts and ownership of data shall follow the users' funding agreement and/or the organisation's policies.

F.2 Notwithstanding the foregoing, the user agrees that to benefit the Cybersecurity community, NCL shall have the right and be entitled to use the IP and to collect useful reusable data objects to further enhance the NCL infrastructure as well as to support future experimentation.

F.3 For projects receiving funding from the government, with agreement that the government has the right to use the artifacts or data created, the project leader shall procure from the funding agency permission/approval from the funding agency to allow hosting of artifacts or data in the testbed for re-use by the community and NCL.

F.4 Users shall consent to the collection by NCL of users' data and the meta-data of their projects and experiments for resource management and audit purposes, this information will be managed according to the Personal Data Protection Act. NCL will use commercially reasonable effort to ensure the security and integrity of the data.

F.5 For projects from the local RIs, AUs, IHLs, the project leader shall provide a description of project, a description of the possible data, software, algorithms, or other artifacts that may be re-used, and the contact (email addresses, phone numbers, websites) to inform other users of the potential usage. The project leader shall ensure that the contact is be valid during the project period and three (3) months thereafter and shall promptly give notice in writing to NCL of any changes to the contact particulars.

F.6 If NCL deems that it will have substantial involvement in creating an artifact or producing data in an experiment, NCL will discuss with the user to ascertain the IP ownership of artifacts and ownership of data prior to the commencement of the experiment.

G. Monitoring & Closure

G.1 NCL will monitor the experiments regularly and highlight to the project leader if his/her experiment has not been active for a period of time. The project leader shall end the experiment when there is no further activity required. NCL reserves the rights to end an experiment after issuing to the project leader at least three (3) reminders and the user has failed in NCL's view to provide adequate response or justification against closure of the experiment. . NCL shall not be responsible for data lost as a result thereof and/or in such a manner.

H. Acceptable Use

H.1 A summarised description of acceptable usage is set out below. Please refer to the Subscription Agreement for further details.

H.2 **No Illegal, Harmful, or Offensive Use or Content**

Users may not use, or encourage, promote, facilitate or instruct others to use, the Services or NCL Lab Environment for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive or would constitute a criminal offense or give rise to civil liability, or otherwise use the NCL Environment in a manner which is contrary to law, a violation of third party rights including, without limitation, copyright, rights to publicity and privacy, or would serve to restrict or inhibit any other user from using or enjoying the NCL Environment. Prohibited activities or content include:

a. **Illegal Activities.** Any illegal activities, including advertising, transmitting, or otherwise making available gambling sites or services or disseminating, promoting or facilitating child pornography.

b. **Harmful or Fraudulent Activities.** Activities that may be harmful to others, our operations or reputation, including offering or disseminating fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, Ponzi and pyramid schemes, phishing, or pharming), or engaging in other deceptive practices.

c. **Infringing Content.** Content that infringes or misappropriates the intellectual property or proprietary rights of others.

d. **Offensive Content.** Content that is defamatory, libellous, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.

e. **Harmful Content.** Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.

H.3 **No Security Violations**

Users may not use the Services to violate the security or integrity of any external System. Prohibited activities include:

- **a. Unauthorized Access.** Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
- **b.** Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited
- **c. Interception.** Monitoring of data or traffic on a System without permission.
- **d. Falsification of Origin.** Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

H.4 **No Network Abuse**

Users may not make network connections to any external System unless requisite permission from the NCL AND the party controlling access to that external System is obtained. Prohibited activities include:

a. **Monitoring or Crawling.** Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.

b. **Denial of Services (DoS).** Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.

c. **Intentional Interference.** Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.

d. **Operation of Certain Network Services**. Operating network services like open proxies, open mail relays, or open recursive domain name servers.

e. **Avoiding System Restrictions.** Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

H.5 No E-Mail or Other Message Abuse

Users shall not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like "spam"), including commercial advertising and informational announcements. Users shall not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission. Users are not to collect replies to messages sent from another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

H.6 Monitoring and Enforcement

NUS reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the Services or NCL Site. NUS may:

(1) investigate violations of this Policy or misuse of the Services or NCL Site; or

(2) remove, disable access to, or modify any content or resource that violates this Policy or any other agreement which NUS has with the user for use of the Services or the NCL Site.

NUS may report any activity that that NUS suspects of violating any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties.

NUS reporting may include disclosing appropriate customer information. NUS may also cooperate with law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.