Appropriate Use Policy

VERSION 2021.08.16

You must understand and abide by CNNL's Appropriate Use Policy to use its high-performance computing (HPC) systems.

CNNL HPC Resources

The following is a list of general computer use policies, procedures, and security rules that apply to individual end users of the Computational Nanoelectronics & Nanodevices Lab (CNNL) High Performance Computing (HPC) resources. Principal Investigators are responsible for ensuring that these policies, procedures, and security rules are followed for their organizations and ensuring that HPC users working under their supervision fulfill these responsibilities.

HPC User Accountability

HPC users are accountable for their actions. Violations of policy, procedure, and security rules may result in applicable administrative sanctions or legal actions.

HPC Resource Use

The use of CNNL HPC resources for personal or private benefit is prohibited. The use of CNNL HPC resources to support illegal, fraudulent, or malicious activities is prohibited. The use of CNNL HPC resources to facilitate any transaction that would violate Singapore export control regulations is prohibited.

The CNNL make no express or implied warranty with respect to the use of CNNL HPC resources. CNNL shall be liable in the event of any HPC system failure or loss of data.

Usernames and Passwords

A user identifier (username) and an associated password are required of all CNNL HPC users. Individuals who have a CNNL-assigned user identifier are responsible for protecting the associated password. Passwords must be changed at CNNL's request. Passwords must not be shared with any other person and must be changed as soon as possible after an unacceptable exposure, suspected compromise, or at the direction of CNNL personnel.

Account Usage

HPC users are not permitted to share their accounts with others.

Notification

HPC users must immediately notify eledd@nus.edu.sg or elefongx@nus.edu.sg upon awareness that any of the accounts used to access CNNL HPC resources have been compromised. HPC users should promptly inform CNNL of any changes in contact information.

Upon actual or suspected loss, disclosure, or compromise of the associated password, account holders must immediately notify eledd@nus.edu.sg or elefongx@nus.edu.sg.

Software and Data

CNNL HPC resources are operated as research systems and should only be used to access and store data related to research.

CNNL HPC resources control data access via username and password authentication for network access and UNIX directory and file permissions for data storage. Network access and data storage systems provide no explicit encryption. HPC users are responsible for protecting data files and acknowledge and understand that CNNL's HPC security control implementation is sufficient for research data access and storage.

HPC users must ensure that when using HPC resources that all software is acquired and used according to appropriate licensing. Possession, use, or transmission of illegally obtained software on HPC resources is prohibited. HPC users shall not copy, store or transfer copyrighted software or data using HPC resources, except as expressly permitted by the copyright owner.

Data Retention

CNNL reserves the right to remove any data at any time and/or transfer data to other individuals (such as Principal Investigators working on a same or similar project) after a user account is deleted or a user no longer has a business association with CNNL.

Although CNNL takes steps to ensure the integrity of stored data, CNNL does not guarantee that data files are protected against destruction. HPC users are strongly encouraged to make backup copies of all data and important software.

In some cases, CNNL may elect to make backup copies of some data files. When backup copies are made, CNNL reserves the right, at its sole discretion, to hold such backup copies indefinitely or to delete them.

Deviations from Authorized Privileges Not Allowed

HPC users may not deviate from the terms of this CNNL HPC Appropriate Use Policy in any way, including, but not limited to, the following prohibitions:

Unauthorized Access: HPC users are prohibited from attempting to send or receive messages or access information by unauthorized means, such as imitating another system, impersonating another user or other person, misusing legal user credentials (usernames, passwords, etc.), or causing some system component to function incorrectly.

Altering Authorized Access: HPC users are prohibited from changing or circumventing access controls to allow the user or others to perform actions outside authorized privileges.

Reconstruction of Information or Software: HPC users are prohibited from reconstructing or re-creating information or software outside authorized privileges.

Data Modification or Destruction: HPC users are prohibited from taking actions that intentionally modify or delete information or programs outside authorized privileges.

Malicious Software: HPC users are prohibited from intentionally introducing or using malicious software, including, but not limited to, computer viruses, Trojan horses, or worms.

Denial of Service Actions: HPC users are prohibited from using CNNL HPC resources to interfere with any service availability, either at CNNL, or at other sites.

Pornography: HPC users are prohibited from using CNNL HPC resources to access, upload, download, store, transmit, create, or otherwise use sexually explicit or pornographic material.

Harassment: HPC users are prohibited from engaging in offensive or harassing actions toward another individual or organization.

Monitoring and Privacy

HPC users have no explicit or implicit expectation of privacy. CNNL retains the right to actively monitor all HPC resources, activities on CNNL systems and networks and to access any file without prior knowledge or consent of HPC users, senders, or recipients. CNNL may retain copies of any network traffic, computer files, or messages indefinitely without user's prior knowledge or consent. CNNL may, at its discretion, share information gathered through monitoring with other incident response organizations, and local and international law enforcement organizations.

CNNL personnel and HPC users are required to address, safeguard against, and report misuse, abuse and criminal activities. Misuse of CNNL HPC resources can lead to temporary or permanent disabling of accounts, and administrative sanctions or legal actions.

CNNL APPROPRIATE USE POLICY FOR VERSION 1.2 UNDERTAKING

I have read, understood and accepted the Appropriate Use Policy, version 2021.08.16 set out above, including any revisions to the policy.

Requesting User	
Name:	
Student/Staff No. or Organization:	
Signature:	
Date:	
Supervisor/Cluster Admin (delete where applicable)	
Name:	
Student/Staff No. or Organization:	
Signature:	
Date:	