Zimbabwe

Centre for High Performance Computing (ZCHPC)

HPC Usage Policy

"Creating a secure computing environment"

Table of Contents

1. Definition of Terms

TERM	DEFINITION
High Performance Computer (HPC) or Supercomputer	Refers to a high-tech powerful computing infrastructure that is used to solve large complex computational problems that cannot be solved by an ordinary computer.
HPC Centre	Refers to the Zimbabwe Centre for High Performance Computing (ZCHPC) site that houses the supercomputer resources, specialised infrastructure equipment and personnel.
Infrastructure	Refers to all the HPC Centre hardware and software technical resources such as computing, electronic, electrical, mechanical and security technologies.
Employees/personnel	Refers to people employed by the HPC Centre.
ZCHPC Community	Refers to all personnel, users, guests, clients, partners and vendors.
HPC User	A person who has access remotely or locally to HPC Centre computers, software, networks or any other computing and information technology resources.
User-Id	Also known as accounts, a unique identifier for an HPC User.
Computers	An electronic device that manipulates information or data with ability to store, retrieve, and process data. Computer includes desktop workstations, laptop computers, handheld computing device, servers etc.
Virus	A virus is a form of malicious code and, as such it is potentially disruptive. It may also be transferred unknowingly from one computer to another. The term Virus includes all sorts of variations including macro-viruses, Trojans, and Worms.
Antivirus	Software designed to detect and destroy computer viruses.
Malware	Malicious software designed to damage or infiltrate a computer system without the owner's informed consent.
Spam	Unsolicited e-mail or news posts usually sent to a multiple accounts at the same time.

Trojan	This is malware that appears to perform a desirable function, but in fact performs undisclosed malicious functions.
Authorisation	Official permission or approval. Authorisation could be in written or electronic format and this should be stored for at least the duration of the requirement.
Authorised Use	Actions that employee or user are expressly permitted to do as part of their job function and / or reasonable use of IT facilities.
Confidential and Sensitive Information	A designation for information, the disclosure of which is expected to negatively impact on the organisation, its clients, partners or vendors.
Electronic Identity	This refers to all aspects of a user's HPC Centre electronic persona or characteristics, including username, password (credentials), e-mail address, chat or messenger address and all systems to which this may apply.
Unsolicited Communications	Communications sent to a recipient who neither wants nor is requesting such communications.

2. Introduction

The High Performance Computing Centre is about people, organizations, institutions, products and technologies connected through cyber space domain by interconnected telecommunications infrastructures. The HPC Usage Policy is a **Sector Specific Cyber Security Policy** meant to safeguard the Zimbabwe Centre for High Performance Computing (ZCHPC) technical resources against abuse. It outlines the expected best practice and behaviour by the Users. The Policy defines general conduct, usage of resources, handling of equipment and penalties associated in breaching the Policy. The HPC Users are obliged to agree to be bound by the Policy before accessing any ZCHPC resources.

3. Purpose

This Policy defines the minimal acceptable use of ZCHPC infrastructure and information by its Users. The Policy protects the ZCHPC Information infrastructure credibility, reputation, privacy and rights of the Users. Furthermore, this Policy will help in ensuring that resources are available for the primary business purpose, without being impacted by non-business or abusive behaviours. Finally, this Policy endeavours to provide a safe and enjoyable working environment for all personnel, free from all forms of physical abuse, electronic abuse and misuse through ensuring;

- Confidentiality of information from unauthorized disclosure;
- Integrity of information from unauthorized modification;
- Availability of information when it is required.

4. Objective

The primary focus of this Policy is to:

- Promote the provision of accessible, universal, affordable, reliable high end computing facilities and services.
- Provide for the creation of an enabling legal and regulatory environment that ensures safe usage, growth and development of the HPC Infrastructure.
- Promote the use of computational and storage resources in improving national research and innovation capability so as to build a growing research-savvy nation.

5. Audience

This Policy is applicable to all HPC Centre Users using the Centre Infrastructure. The Policy is also applicable to all Users regardless of their location, i.e. working from the HPC Centre or remotely.

6. Enforcement

It remains the primary responsibility of Centre personnel for the administration and enforcement of the Policy.

Violation of this Policy can lead to misconduct charges, legal action or termination of contract. In some scenarios this failure may also constitute a criminal offence and it will be dealt with by the law enforcement agencies.

Furthermore, failure to comply with this Policy may result in partial or complete termination or restriction of access rights to the HPC Centre infrastructure and services through. HPC Centre will endeavour to advise it's users on any Policy changes. However responsibility rests with the user to ensure that they are aware of, and fully understand the Policy.

7. General Policy

7.1 General Use, Ownership and Practice

7.1.1 General Conduct

1. Users shall not access computers, software, information or any network resource without authorisation.
2. Users shall not transmit, store, process, distribute, use or view any information considered abusive, pornographic, distasteful, threatening, libellous, hateful or in contravention of local, common law, state, national or International laws.
3. Users shall not capture or reproduce any processes or information belonging to ZCHPC customers, partners or vendors, including taking photographs, photocopying or scanning of documents without prior permission being granted.
4. Users shall not violate the rights of any person, protected by the laws regarding copyright, trade secrets, patent or any other intellectual property or similar rights or regulations.
5. Users shall not transmit any company information for any unauthorised purpose, regardless of whether it is restricted or not.
6. Users shall not restrict or inhibit any person, whether an employee, client, partner or vendor of HPC Centre or otherwise, in his or her authorised use of HPC Centre's systems, services or products.
7. Users shall not furnish false information on any form, contract or application, including the fraudulent use of credit card numbers and personal identification information.

7.1.2 Use of HPC Centre Resources

1. Always run only the standard anti-virus software provided by the ZCHPC.
2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
3. Never open any files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.
4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
5. Files with the following filename extensions are blocked by the e-mail system: [list extensions]. [Describe any workaround procedures for sending/receiving business-critical files with banned extensions, such as use of a file compression utility.]
6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
7. Avoid direct disk sharing with read/write access. Always scan your flash drives for viruses before using it.
8. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
9. Back up critical data and systems configurations on a regular basis and store backups in a safe place.
10. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.
11. Access to the internet through ZCHPC computers or networks is provided primarily for business purposes.

7.1.3 General Equipment Care and Safety

1. Users are responsible for the good care and condition of all HPC Centre equipment assigned to their use. Computers are sensitive to extreme temperatures. This includes external hard drives, CD-ROMs, batteries, etc. Safeguard equipment appropriately during times of extreme heat and cold.
2. ZCHPC will not be held liable for any loss incurred on personal equipment within the Centre or loss of data resulting from user negligence.
3. Users will be held accountable for the repair or replacement costs of any equipment, due to the user's negligence, is damaged or lost while using the Centre facilities.

7.1.4 Physical Security or Access Control.

1. Access Tags: All Users shall be allocated individual access tags for entry into the HPC Centre. These tags must be exchanged with their national identification cards on entry and exit point. These tags should never be shared among the Users.
2. Daily usage of access tags is governed by the **Access Tag Guidelines** document to be signed upon receipt of the access.
3. Visitors to the Centre must register their electronic machines with the security personnel at entry/exit check point.
4. HPC users at the Centre are restricted only to the user cubicle room or any specifically assigned working space and any queries must be directed to either the reception or the security check point.
5. Users are not permitted beyond the Technical Division areas that includes Server Room, CCTV Control Room, UPS Room, Transformer House, Technical Offices and Technical Passages.
6. Food and alcohol is not allowed inside the user cubicles for users who shall be accessing the system at the Centre.
7. Loitering is not allowed at the Centre.
8. For the purposes of other users keep any conversations to a minimum and make sure that all cell phones are put on silent in the user cubicles.
9. Bags and parcels are subjected to security check at both entry and exit points.
10. Motor vehicles are subject to security check at both entry and exit points.

7.2 Security of Proprietary or Sensitive information

HPC Users might encounter information that is sensitive or confidential and it is expected that every user has an awareness and understanding of the value of such information.

Users shall endeavour at all times to protect the proprietary and confidential information of ZCHPC, its clients, partners and vendors. Information shall only be made available to those authorised to view or access it. Information shall be protected according to its level of confidentiality and sensitivity.

7.3 System and Network Use

Account Administration-In order to use the supercomputer, users must get an account which consists of a username, password, and disk space to store files. From that account, users are discouraged to run their jobs on the login node. Users must approach the HPC Centre for the opening of HPC Usage Account.

Users who shall be accessing the HPC physically at the Centre might be given a network access key for the Internet usage. By using the ZCHPC wired or Wi-Fi internet access service, you represent and agree that you are a guest of the ZCHPC.

7.3.1 Unacceptable or Prohibited Use

The following activities and practices shall be considered **strictly unacceptable**:

Unacceptable actions that should NOT be done with your HPC account and HPC Centre resources include;

1. Transferring music, video, images or other files for personal use.
2. Sharing files with your friends.
3. Anything that is a violation of a software license agreement. The software license agreements are in the documentation directory for any software installed on the HPC systems.
4. Any other illegal activity, such as hacking into computer systems you are not authorized to use.
5. Connection of non HPC devices without prior clearance by the HPC Personnel.
6. Violation of the rights of any person or organisation protected by copyright, trade secret, patent or other form of intellectual property or similar laws or regulations. This includes, but is not limited to the installation of pirated or other software products not licensed for use by HPC Centre.
7. Unauthorised copying of any copyrighted material, including but not limited to photographs from magazines, books or other copyrighted sources, copyrighted music, movies or copyrighted software for which ZCHPC or the end user does not have a valid license.
8. Exporting software, technical information, encryption software or technology in violation of any international or regional or local export control laws.
9. The introduction of malicious programs onto the network, including viruses, Trojans, worms, e-mail bombs and other forms of malware.
10. Revealing your account access details (username, password) to others or allowing the use of your account or identity by others, including colleagues, family and friends.
11. Using ZCHPC 's computing resources to engage in procuring or transmitting any material that is in violation of workplace laws, including those pertaining to sexual harassment, workplace hostility and others defined under local jurisdiction.
12. Making fraudulent offers of any products, services or items, originating from ZCHPC computer resources or accounts.
13. Causing or facilitating security breaches or disruptions to ZCHPC infrastructure and networks. Security breaches include, but are not limited to:
    a. Accessing data for which the user is not the intended or authorised recipient
    b. Accessing computer resources for which the user is not expressly authorised to access
    c. Causing network disruptions, through the actions of network sniffing, ping floods, packet spoofing, denial of service and other malicious actions
14. Circumventing the security controls of any host, network, service, server or account.

7.3.2 Corporate and Personal Computer Software

Unacceptable actions include:

1. Installing softwares or making copies of any software (or similar copyrighted materials) on HPC Infrastructure without the explicit permission of the Centre Personnel.
2. Copying of HPC Centre licensed softwares.

7.3.4 Security System

Unacceptable actions include:

1. Tempering with access control, CCTV and fire control devices.
2. Obstructing security personnel from executing their duties.
3. Physical access to restricted places.

7.3.5 User Accounts

Unacceptable actions include:

1. Accessing another user's account without explicit permission.
2. Making known account details to users not authorised to have those details.
3. Consuming excessive resources, including CPU time, memory, disk space, and session time for personal use, including use, viewing, accessing, transmission, distribution, or storage of any material which is not HPC usage related such as pornographic or undesirable.
4. The use of resource-intensive programs, which negatively affect other system users, or the performance of HPC Centre systems or networks.
5. Accessing or copying someone else's files or programs, unless explicitly authorised to do so by the information owner.
6. Attempting to circumvent computer, account or operating system security.
7. Disabling security software on HPC Centre computers, network devices or servers, including antivirus software, antispyware software, firewall software or any other security components.

7.3.6 Electronic Communications (E-mail, Instant Messaging, Chat)

Unacceptable actions when using the HPC Centre Infrastructure include:

1. Copyrighted material: Sending or sharing unauthorized copyrighted materials electronically.
2. Intimidation: Sending electronic communication that is abusive or threatens an individual in any manner.
3. Harassment: Using electronic communications to harass an individual in any manner, including sending or forwarding chain letters, deliberately flooding a user's mailbox with automatically generated mail or chat messages, and sending messages that are deliberately designed to interfere with normal electronic communications delivery or access. All forms of harassment,

whether through language, frequency, or size of messages, are strictly prohibited.

4. Unsolicited communications: Sending or initiating unsolicited electronic communications including the sending of "junk mail" (e-mail spam) or other advertising material to individuals who did not specifically request such material. It is prohibited to send unsolicited bulk mail or chat messages or to make unsolicited posts to social networking sites. This includes, but is not limited to, bulk mailing of commercial advertising, informational announcements, and political tracts. Such material may only be sent to those who have explicitly requested it. If a recipient asks to stop receiving e-mail or messages, then the user shall not send that person any further electronic communications. This does not apply to normal business information communications.
5. Malicious communications: Engaging in malicious communications, including, but not limited to, "mail bombing" (flooding a user or site with very large or numerous e-mails), posting of derogatory comments and spreading mis-information.
6. Forged / Spoofed e-mail: Forging an electronic mail signature or address (mail headers) to make it appear as though it originated from a different person. This does not apply to the normal business practice where an assistant or secretary replies on behalf of someone else.

7.3.7 Social Networking

Social Networking sites include, but are not limited to MySpace, Blogger, YouTube, Yahoo groups, MSN groups, Xanga.com, ANobii, Flickr and Facebook.

Unacceptable actions using HPC Centre communications channel include:

1. Misrepresentation: Speaking on behalf of ZCHPC or making comment on matters relating to ZCHPC.
2. Harassment: Using social networking communications channels to harass an individual in any manner. All forms of harassment, whether through language, frequency, size or type of communication, are strictly prohibited.
3. Unsolicited communications: Sending unsolicited electronic communications to other individuals via any communications channel related to social networking interactions.
4. Unauthorised access: Attempting to gain access to another person's social networking account, profile or files regardless of whether the access was successful or whether the information accessed, involved personal information.
5. Copyrighted material: Making unauthorized copyrighted materials available via social networking channels.
6. Undesirable material: Accessing, copying or downloading any generally undesirable material, including, but not limited to, pornography, discriminatory or hate sites.

7.3.8 Remote Access

Unacceptable actions include:

1. Making use of ZCHPC remote access to access, copy or send any undesirable material, including but not limited to spam, pornography, abusive or copyrighted material.

7.4 Monitoring and Disclosure

1. All Electronic communications directed to or originating from ZCHPC shall be monitored and logged, scanned for anyone else making use of its infrastructure and resources for possible malware and for any offensive material.
2. ZCHPC reserves the right to monitor the electronic communications Electronic communications utilising ZCHPC infrastructure and resources are considered business records and may be subpoenaed by a court of law.
3. ZCHPC will store, access, monitor and disclose the contents of electronic communications to assure system security comply with company Policy or comply with requests by a court of law.

7.5 Complaints and Queries

Complaints, concerns or queries regarding any aspect of the acceptable use Policy can be addressed to the Chief Executive Officer/Director or the Technical and Operations Manager.

8. Policy Revision

The ZCHPC reserves the right to amend this Policy from time to time and without prior notice. Any such modifications shall be automatically effective and shall be deemed to have come to the attention of all users when posted to the ZCHPC website.

9. Declaration of Understanding

I……have read, understand and agree to adhere to the HPC Usage Policy. I also agree that the ZCHPC may, at any time and for any reason, change, terminate, limit or suspend my access to this service and upon termination my rights to use this service will immediately cease. The ZCHPC also reserves the right to revise this agreement at any time without prior notice, and I agree that the ZCHPC may do so.

Title	: Hon/Prof/Dr/Mr/Mrs/Miss ……
Institution	:……
Designate	:……
EC / ID Number	:……
Date	: ……
Signature	: ……

Forward a signed Policy Document to the mailto:helpdesk@zchpc.ac.zw

For further enquiries kindly contact us at:

Website: www.zchpc.ac.zw

Contact Numbers: +2634334420 or +2634334895

END