



<b>CHPC Use Policies</b>			
Document no	DMS ref no		
Revision status	0.1		
Author	Khomotso Kganyago		
Publication date	21 April 2008		
Approval by		Management	Board Representative (if required)
Name			
Signature			
Date			

## TABLE OF CONTENTS

<a href="#"><u>1 DOCUMENT CHANGE HISTORY.....</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>2 INTRODUCTION.....</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>3 CHPC OBJECTIVES.....</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>4 USER ACCOUNTABILITY.....</u></a>	<a href="#"><u>4</u></a>
<a href="#"><u>5 RESOURCE USE.....</u></a>	<a href="#"><u>4</u></a>
<a href="#"><u>6 SOFTWARE USE.....</u></a>	<a href="#"><u>4</u></a>
<a href="#"><u>7 PASSWORDS AND USERNAMES.....</u></a>	<a href="#"><u>4</u></a>
<a href="#"><u>8 NOTIFICATION.....</u></a>	<a href="#"><u>4</u></a>
<a href="#"><u>9 UNAUTHORIZED ACCESS.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>10 ALTERING AUTHORIZED ACCESS.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>11 RECONSTRUCTION OF INFORMATION OR SOFTWARE.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>12 DATA MODIFICATION OR DESTRUCTION.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>13 MALICIOUS SOFTWARE.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>14 DENIAL OF SERVICE ACTIONS.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>15 DATA RETENTION.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>16 ACCOUNT USAGE.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>17 MONITORING AND PRIVACY.....</u></a>	<a href="#"><u>5</u></a>
<a href="#"><u>18 ACRONYMS.....</u></a>	<a href="#"><u>6</u></a>
<a href="#"><u>19 OWNERSHIP AND RESPONSIBILITIES.....</u></a>	<a href="#"><u>6</u></a>
<a href="#"><u>20 SIGN AND RETURN TO CHPC.....</u></a>	<a href="#"><u>7</u></a>

## 1 DOCUMENT CHANGE HISTORY

PUBLICATION DATE	AUTHOR	REVISION NO.	CHANGE DESCRIPTION
June 2007	Khomotso Kganyago	0	
21 April 2008	Jeremy Main	0.1	<ul style="list-style-type: none"><li>● Changed Fax number</li><li>● Add servicedesk@chpc.ac.za as return address.</li><li>● Formatting: bullet 20 to one page.</li></ul>

## 2 Introduction

The following is a list of general computer use policies and security rules that apply to all users of CHPC resources. Further information on CHPC security policies and practices can be found at <http://www.chpc.ac.za/security/>. CHPC must have a signed copy of this form on file for every user.

## 3 CHPC Objectives

The Vision of the CHPC is planned to be achieved in 5 years, with the start- up phase being finalized in the next 2 years, and the following 3 years focusing on consolidation and growth. Targets and measures will be organized within DST's basket-of-measures, which include:

- Human Resource Development (such as transformation, Black and Female Scientists, outreach efforts, numbers of M.Sc and PhD students and post-doc fellowships),
- S&T excellence (such as publications in international peer-reviewed journals, hosting an international scientific conference),
- Innovation and Learning (such as peer review and benchmarking as part of a learning process),
- Customers and Stakeholders (such as customer and partner usage of the CHPC, government support),
- Finance and Investment (such as achieving commercial income targets, adherence to budget), and
- Operational excellence (such as world-class project management and research processes).

The CHPC will need to focus on the following key issues on an ongoing basis in order to accomplish its vision:

- Effective governance
- Development of nodes and partnerships with TEI's, research institutes and industry, locally, nationally, in the rest of Africa, and internationally (particularly with developing countries)
- Human resource development, transformation, capacity development, and training
- Ensuring funding sustainability via government core funding as well as from commercial beneficiaries
- Developing a critical mass in HPC and people

- In partnership mode, do a range of relevant and research projects with impact and visible S&T outcomes
- Provide appropriate support to the nodes and partners
- S&T excellence and an effective research plan
- On an ongoing basis ensure (with government and SANReN support), sufficient and affordable bandwidth
- Develop and implement cutting-edge computational tools
- Effective and focused marketing, including contributing to public understanding of S&T

#### **4 User Accountability**

Users are accountable for their actions and may be held accountable to applicable administrative or legal sanctions.

#### **5 Resource Use**

Computers, software, and communications systems provided by CHPC are to be used only for work sanctioned by the Scientific Advisory Committee and CHPC Management. Use of CHPC resources to store, manipulate, or remotely access any national security information is prohibited. The use of CHPC resources for personal or non-research-related activity is prohibited. CHPC systems are provided to our users without any warranty. CHPC will not be held liable in the event of any system failure or loss of data.

#### **6 Software Use**

All software used on CHPC computers must be appropriately acquired and used according to the appropriate licensing. Possession, use or transmission of illegally obtained software is prohibited. Likewise, users shall not copy, store or transfer copyrighted software or data, except as permitted by the owner of the copyright.

#### **7 Passwords and Usernames**

A user identifier known as a username and password are required of all users. Passwords must be changed at least every six months. All passwords must conform to CHPC guidelines which can be found at the CHPC website. Passwords must not be shared with any other person and must be changed as soon as possible after an unacceptable exposure, suspected compromise or by direction of a CHPC staff member.

#### **8 Notification**

Users must notify CHPC immediately when they become aware that any of the accounts used to access CHPC have been compromised. Users should promptly inform CHPC of any changes in their contact information.

## **9 Unauthorized Access**

Users are prohibited from attempting to receive unintended messages or access information by unauthorized means, such as imitating another system, impersonating another user or other person, misuse of legal user credentials (usernames, passwords, etc.), or by causing some system component to function incorrectly.

## **10 Altering Authorized Access**

Users are prohibited from changing or circumventing access controls to allow themselves or others to perform actions outside their authorized privileges.

## **11 Reconstruction of Information or Software**

Users are not allowed to reconstruct or recreate information or software for which they are not authorized.

## **12 Data Modification or Destruction**

Users are prohibited from taking unauthorized actions to intentionally modify or delete information or programs.

## **13 Malicious Software**

Users must not intentionally introduce or use malicious software such as computer viruses, Trojan horses, or worms.

## **14 Denial of Service Actions**

Users may not deliberately interfere with other users accessing CHPC or other system resources.

## **15 Data Retention**

CHPC reserves the right to remove any data at any time and/or transfer data to other individuals working on the same or similar project once a user account is deleted or a person no longer has a business association with CHPC. This will be done in consultation with the leader of the project, in case there might be IP issues associated with the project, as stipulated in the Memorandum of Agreement between the CHPC and Project's Institution or Organization.

## **16 Account Usage**

Users are not allowed to share their accounts with others.

## **17 Monitoring and Privacy**

Users have no explicit or implicit expectation of privacy. CHPC retains the right to monitor the content of all activities on CHPC systems and networks and access any computer files without prior knowledge or consent of users, senders or recipients. This exercise will be done responsibly

considering the confidentiality of the information. CHPC may retain copies of any network traffic, computer files or messages indefinitely without prior knowledge or consent. CHPC personnel and users are required to address, safeguard against and report misuse, abuse and criminal activities. Misuse of CHPC resources can lead to temporary or permanent disabling of accounts, loss of allocations, and administrative or legal actions.

## 18 Acronyms

Acronyms	Description of meaning
SAC	Scientific Advisory Committee
CHPC	Centre for High Performance Computing
ICT	Information and Communication Technology
TEI	Tertiary Education Institution
S&T	Science and Technology
IP	Intellectual Property
DST	Department of Science and Technology

## 19 OWNERSHIP AND RESPONSIBILITIES

The Technical Operations Manager will be responsible for updating this document from time to time if required, and also for the implementation and the management of compliance issues associated with this document.

## 20 Sign and return to CHPC

By FAX (preferred): (021) 658 2744

By Email :servicedesk@chpc.ac.za

By Postal Service: CHPC Account Support, 15 Lower Hope Road, Rosebank, Cape Town, 7700

Project Name: \_\_\_\_\_

Project Leader: \_\_\_\_\_

Project Member: \_\_\_\_\_

Citizenship: \_\_\_\_\_

Organization: \_\_\_\_\_

Email Address: \_\_\_\_\_

Work Phone Number: \_\_\_\_\_

Alternative Phone Number (e.g. Cell/Mobile): \_\_\_\_\_

CHPC Technical/Scientific Officer for one of your CHPC project accounts (repositories):

\_\_\_\_\_

***I have read the CHPC Policies and Procedures and understand my responsibilities in the use of CHPC resources.***

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Approved	
Not Approved	

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Remarks: