Computing Usage Policy

Document no: 22670

Revision no: 2.0

Date: 11 August 2014

Supported by Australian Government State Government Victoria

Synchrotron Light Source Australia Pty Ltd ABN 18 159 468 256 ACN 159 468 256 www.synchrotron.org.au
800 Blackburn Road, CLAYTON, VIC, 3168 **p** +613 8540 4100 **f** +613 8540 4200

REVISION HISTORY

Revision	Date	Prepared by	Description
0.0	25/01/2013	Uli Felzmann	Initial draft
	06/02/2013	Uli Felzmann	Implemented suggestions from Dean Morris
0.1	06/02/2013	Snezana Vukovic	KnowledgeTree upload
0.2	06/02/2013	Snezana Vukovic	Document properties update
1.0	12/03/2013	Snezana Vukovic	KnowledgeTree release
1.1	06/03/2014	Kathleen Riches	Re-format and restructure to new policy format.
1.2	15/03/2014	Uli Felzmann	Clarifying email usage, prohibited activities. Fixing typos.
1.3	13/05/2014	Uli Felzmann	Addressing comments from Angela Friedrich, Senior Administrative Lawyer, ANSTO.
1.4	28/06/2014	Uli Felzmann	Clarifying “Ownership and compliance” after feedback from the ERF was received.
2.0	11/08/2014	Snezana Vukovic	KnowledgeTree release

TABLE OF CONTENTS

1 PURPOSE

This document sets out Synchrotron light Source Australia's (SLSA) policy in relation to the use of the SLSA computing facilities.

The SLSA computing facilities are intended to be used for SLSA purposes and for the attainment of the SLSA's aims. Your use must be for official work purposes and must not cause any damage to SLSA (including reputational damage), nor disrupt its operation. Further, your use must not be for any activity that is illegal under local, state, federal or international law.

Any improper or malicious use of the SLSA computing facilities may cause damage to the SLSA (including reputational damage), and serious problems for other users of these facilities and may jeopardize computer security at the SLSA.

2 SCOPE

This policy applies to all employees of Synchrotron Light Source Australia (SLSA), contractors and all users of SLSA computing facilities.

3 RELATED AND SUPPORTING DOCUMENTS

The following documents should be read in conjunction with this policy as they relate to, and provide support for, the application of this policy:

Document No.	Document Title
13016	Code of Ethics Policy
24219	Computing Security Policy
14174	Media Policy

4 DEFINITIONS

For the purpose of this policy, the term "SLSA computing facilities" is defined as:

- all personal computers, work stations, mobile devices, servers and peripheral systems such as printers, on the SLSA site and directly or indirectly connected to any SLSA network;
- all applications running on or related to any of the computers and above-mentioned networks, and all electronic mail, intranet and Internet services supported by the SLSA computing facilities;
- all parts of the SLSA information system network.

For the purpose of this policy, the term "user" means any person making use of the SLSA computing facilities.

5 ROLES AND RESPONSIBILITIES

Unless otherwise stated, the Group Leader – Scientific Computing and IT, is responsible for maintaining this policy on behalf of the Head of Science.

All Managers are responsible for implementation and compliance monitoring of this policy in their work areas.

All employees, contractors and all other users of SLSA computing facilities are responsible for complying with this policy.

6 POLICY DETAILS

6.1 Access to accounts and data

Accounts, whether single or shared access, may only be used for the purpose for which they have been allocated to the user.

All accounts must have appropriate access protection. The user shall protect details of their personal account, particularly by avoiding obvious passwords and shall not reveal passwords to any third party. The user must keep confidential all information obtained from access to the SLSA computing facilities that the user should reasonably expected is confidential or sensitive in nature. The user must not seek unauthorized access to accounts which have access protection and must not, except if otherwise approved, look for, disclose or exploit any security weaknesses in the SLSA computing facilities or use these facilities to do so with respect to any other computing facilities.

Users must respect the proprietary rights of SLSA and third parties related to SLSA computing facilities, including software copyright.

6.2 Emails

An email address is provided for every user. Emails sent for work purposes must be sent from the SLSA address. External emails to media organisations must be dealt with in accordance with the SLSA Media Policy.

If there is a genuine business case, and only with prior approval from the Group Leader – Scientific Computing and IT, emails may be sent and received using another account of a partner organisation (ANSTO, CSIRO, Australian Universities, etcetera). Accounts provided by free email providers (Gmail, Yahoo! Mail, etcetera) must not be used as these providers usually reserve the right to use and disclose any information obtained from stored emails.

Other than in the execution of technical responsibilities, the Scientific Computing & IT group employees will not read emails nor grant permissions to others to read emails from personal allocated accounts unless approved by the owner of the email account or approved by the Facility Director. In the event of an employee leaving, an email account may be transferred to their inline manager or another employee in order to complete unfinished tasks.

All use of email and internet facilities is capable of being blocked, intercepted, viewed, actioned and stored by SLSA. By using SLSA's email, internet and intranet facilities, you consent to SLSA viewing and storing all personal information, which you send or receive.

6.3 Standard office environment and customisation

The Standard Office Environment (SOE) is provided in order to allow users to best fulfil their duties. This SOE evolves over time as updates to operating systems and applications occur.

In the event of a failure of the environment, the desktop system may be reset to the current SOE. Addition of freeware programs to the SOE is permitted, but SLSA support for these programs will not offered. The use of shareware programs beyond the conditions of the shareware and the installation of full version software not legally obtained is not permitted.

6.4 Data storage and backup

Essential or irreplaceable data must not be kept on local drives. Only networked shares, which are provided for work related data, are backed up, generally with an overnight process. Data on network shares should be cleaned up on a regular basis and should be kept reasonably structured.

Document management and version control systems such as KnowledgeTree or Perforce are also provided.

Large files such as non-work related movies, files of copyright content such as e-book files, or audio such as MP3 or similar must not be kept on network shares. SLSA may delete such files without warning. This includes the personal network shares.

You must take steps to ensure that data worked on is properly stored, filed and backed up in accordance with the value of the data to the workplace. Managers must check the data storage and backup practices of employees and contractors.

6.5 Ownership and compliance

All material produced by users in their official capacity is owned by the SLSA. Emails sent or received using the SLSA email system are the property of SLSA.

Email messages sent or received by users acting in their official capacity using the SLSA email system are public records and must be managed in accordance with relevant standards.

Any use of the SLSA computing faculties may be monitored and recorded for compliance or security reasons. However, investigations are only initiated on the instruction of the Facility Director.

In particular, SLSA reserves the right to:

- Intercept, view, action, store, disclose and/or prevent the delivery of email messages sent from or received by the SLSA email system (both external and internal);
- Monitor the network activity of staff including web sites visited by staff and emails sent or received by staff;
- Prevent access to any website; and
- Inspect and take action in respect of any files stored in any part of the SLSA computing facilities.

6.6 Rules for personal use

Email is available for legitimate business purposes. A limited amount of personal use is permitted but it must not interfere with the performance of work by staff. Please remember that no privacy or confidentiality attaches to any email, including personal emails sent or received by the SLSA email system. Your use is your consent to the collection and viewing of personal information by the SLSA.

Limited personal use of the computing facilities is tolerated or allowed provided:

- Users are exercising good judgment regarding the reasonableness of personal use.
- It is in compliance with the present policy and does not interfere with official duties including those of others.
- The frequency and duration is limited and there is a negligible use of SLSA resources.

- It does not constitute a political, commercial and/or profit-making activity.
- It is not inappropriate or offensive
- It does not violate applicable laws.

Prohibited activities would include but are not limited to:

- Any intentional disruption of the SLSA computing facilities.
- Unreasonable or excessive personal use during work hours, which interferes with work requirements or workplace productivity.
- Deliberately accessing inappropriate or offensive sites, including but not limited to gambling or sexually explicit sites, and/or printing and distributing such material.
- Undertaking peer-to-peer (p2p) file sharing without the permission from the Group Leader – Scientific Computing and IT.
- Unauthorised copying of copyright material including, but not limited to, digitisation and distribution of photographs from magazines, movies, books or other copyright sources
- Engaging in procuring or transmitting material that could be considered as sexual harassment or workplace harassment.
- Knowingly introducing malicious programs such as viruses into the SLSA network.
- Breaching security including, but not limited to, accessing data of which the employee is not an intended recipient.
- Executing any form of network monitoring, which will intercept data not intended for the employee's host.
- Circumventing user authentication or security of any host, network or account. Interfering with or denying service to any user other than the employee's host.
- Port scanning or password cracking with the intention to break into systems or accounts.
- Making fraudulent offers of products, items or services originating from any SLSA account.
- Exporting software, technical information, or other technology in violation of international or regional export control laws.

7 COMPLIANCE

In the event of a policy breach the incident should be reported to the Head of Corporate Services. Failure to comply with this policy may result in disciplinary action.

8 FURTHER INFORMATION

For further information on any aspect of this policy, please contact the Group Leader – Scientific Computing and IT.