IT Network Access, Data Storage, Email and Internet Policy (April 2012)

Background

SVI computers and computer systems, including internet and email, are resources made available for the effective conduct of scientific research, communication and related administration. Security of the network and safe dissemination and storage of data and other information is critical to the functioning of the organisation.

Responsible use of the facilities includes an undertaking by all users to comply with all procedures to maintain the integrity of the system, including limiting personal use.

Electronic information is regarded the same as any other type of business record, information email or file; as such, SVI reserves the right to access any stored data, and to periodically monitor the volume and content of electronic material accessed and transmitted.

As SVI uses the University of Melbourne computer network, users must abide by the relevant University regulations. The current University regulations (8.3R2) form the basis of this policy.

Purpose

The purpose of this policy is to establish a framework for the use of computer facilities which, as far as possible ensures that the –

- rights of all users are respected
- computer facilities and related resources are used for the purposes for which they are intended and authorised by SVI
- security and integrity of the facilities are not weakened or compromised
- facilities are used in a way which complies with all relevant laws, internal policies, and contractual obligations governing the use of the facilities
- staff, students and visitors of SVI are aware of their obligations with respect to SVI computer services.

Scope

This policy applies to all employees, contract workers, students and volunteers at SVI.

Policy

Network Access

No person may use the network facilities without:

- Obtaining the permission of SVI
- Agreeing to abide by these conditions of use
- Completing an Intellectual Property Agreement.

Connection of Equipment to the Network

- Connection and disconnection to/from the Network is entirely at the discretion of the Cluster IT Support Unit.
- All equipment must provide an authentication mechanism, such as a username and password, and comply with auditing requirements.
- A breach of these conditions of use may result in disconnection from the network.

Responsibilities of Users

- Network facilities may only be used for authorised purposes.
- As email is the primary form of internal communication at SVI, all account holders are required to regularly check their SVI email accounts for important messages and information.
- No user may engage in any act or practice, or omit any act or practice, that constitutes a misuse, as defined in the attached **Misuse Schedule.**
- All users have a responsibility to exercise due care and diligence in the management and maintenance of computing equipment in their care, to prevent that equipment from interfering with the equipment, work or security of others.
- Passwords are provided to individuals for their sole use. Users may not allow any other person to use them without the written approval from SVI. Unauthorised disclosure or sharing of a password or other authentication method is deemed misuse.

Monitoring

- Use of the network may be monitored by authorised persons.
- From time to time authorised persons may examine or monitor network and computer records and logs for operational, maintenance, compliance, auditing, security or investigative purposes.
- Use of the network is provided on the condition that it is agreed that the network is monitored in accordance with this policy. Usage of the network constitutes the consent to monitoring in accordance with this policy.
- SVI reserves the right to monitor and inspect any or all personal and business related internet activity, and to inspect any communication sent or received in order to identify inappropriate use and to protect the organisation, individuals, and/or the system's security and performance.

Confidentiality

- Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of the network, users must be aware that this security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

University of Melbourne Regulation 8.3R2 is located at
http://www.unimelb.edu.au/ExecServ/Statutes/pdf/r83r2.pdf.

Computer and network misuse schedule

Users may not:

a. Use the facilities for any purpose other than authorised purpose.
b. Use the computer systems in any way that would breach any State or Federal law, or would breach SVI policies – Code of Conduct, Equal Employment Opportunity, Confidentiality and Intellectual Property, Privacy.
c. Fail to exercise reasonable care in the use, management and maintenance of the facilities, including hardware, systems and data from theft, unauthorised use or viruses.
d. Create, transmit, store, download or possess illegal material.
e. Visit internet sites, or store, send or receive material that contains offensive, defamatory, illegal, obscene, pornographic, hateful or other objectionable images or material.
f. Use the computer systems for private business, for personal gain or profit, or not;
g. Reveal or publicise SVI confidential or proprietary information.
h. Use the computing facilities for a purpose which constitutes an infringement of copyright.
i. Use the computing facilities for a purpose which would be actionable under law of defamation.
j. Deliberately or recklessly undertake activities that result in unreasonable burden on the facilities, corruption or disruption to data of another or the facilities, disruption to other users, introduce or transmit a virus.
k. Divulge a unique password to any other party without approval, fail to take care to protect a password, or allow unauthorised use of the computing system by another party.
l. Use computer consumables e.g. printers, paper etc. for excessive, personal or otherwise wasteful purposes.
m. Use the computing facilities to annoy, harass or intimidate another person.
n. Use the facilities to gamble on-line, other than participation in approved socially based competitions, such as footy tipping.
o. Circumvent user authentication or access control mechanisms, security including the unauthorised distribution or tools for compromising security, including but not limited to password guessing programs, cracking tools etc.
p. Use the facilities to access unauthorised information including but not limited to unauthorised access to servers, hard drives, email accounts or files.
q. Fail to comply with the conditions of use imposed by an external provider when that provider's facilities or services are used in conjunction with any facilities.
r. Use organisation logos without authorization.
s. Use the facilities to send junk mail or unsolicited bulk messages without approval, send spam, for- profit messages, or chain, hoax or scam messages.
t. Download material that has the effect of impeding the efficiency or safety of the network internet and email services.
u. Download streaming technologies, such on-demand movies, iTunes, peer-to-peer file sharing software eg Kazaa, Limewire, iMesh, Skype.
v. Knowingly run, install or distribute a program intended to damage, compromise the functioning of the facilities, including but not limited to trojan horses, computer viruses, worms.

w. Use the electronic resources for personal use for periods that exceed reasonable limited use. Reasonable limited use means that it is brief and infrequent, and not at the expense of work priorities, and ideally takes place during personal time.

x. Access social networking sites such as *Facebook*, or any other non-work related site, that involves more than a reasonable expenditure of time, or is at the expense of work priorities.

y. Induce, aid or conspire with others to do any of the things referred to in paragraphs (a) to (y).