PROCEDURE FOR POLICY 1.13 – Computing, Technology & Information Resources

Procedures Relating to Security and Privacy of Computing, Information and Technology Resources

1. The university employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the university does not guarantee such security. Users should always engage in "safe computing" practices such as establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

2. The university shall disclose any breach of the security of an information system, following discovery or notification of the breach in the security of the system, to any individual whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the information system.

3. Users should be aware that their uses of university computing resources are not completely private. While the university does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service.

4. For software licenses held by the university, ITS will provide information and clarification around issues of compliance. For all end user or departmentally deployed software, the end user or department is responsible for ensuring compliance.

5. Any computer or network security incident that potentially involves criminal activity shall be reported to Western Special Constable Service.

6. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

RESPONSIBILITIES

7. Everyone who connects a computer to university computing resources has the potential to affect the security of those resources. Everyone must therefore share the responsibility for security. Every employee, contractor, or other worker must understand the university's

Administrator. ITS will help systems administrators carry out these responsibilities to the extent possible with available resources.

7.04 Other Technical Administrators

Others with access to computing resources which involve maintaining electronic administrative

PROCEDURE FOR POLICY 1.13 –

Procedures Related to University E -Mail

1. The university e-

- --

10. Operators of e-mail services have no control over the security of e-mail that has been downloaded to a user's computer. E-mail users should employ whatever protections (e.g., passwords) that are available to them as a deterrent to potential intruders and the misuse of e-mail.

11. E-mail account holders may use their e-mail account for incidental personal purposes provided that such use does not: (1) directly or indirectly interfere with the operation of computing facilities or e-mail services, (2) burden the university with noticeable incremental cost, (3) interfere with the e-mail account holder's employment or other obligation to the university, or (4) contravene this or any other university policy or procedure. E-mail records arising from such personal use may be subject to access as described in the Access and Privacy section of these procedures.

Service Providers & ITS

12.