UNIVERSITY OF TORONTO

INFORMATION + TECHNOLOGY SERVICES

INFORMATION SECURITY GUIDELINES

INFORMATION SECURITY
4 Bancroft Avenue, 1st Floor, Toronto, ON M5S 1C1 Canada
Tel: +1 416 978-7092 • www.its.utoronto.ca/is

TABLE OF CONTENTS:

Simcoe Hall, 27 King's College Circle, Room 5, Toronto, ON M5S 1A1 Canada
Tel: +1 416 978-8385 • Fax: +1 416 978-8903 • cio@utoronto.ca • www.cio.utoronto.ca

APPENDIX 4 - SECURITY BASELINE

Certain practices have become de facto requirements for the protection of data. These practices constitute what is considered to be a managed security baseline:

1. Prompt installation of vendors' software updates to correct known vulnerabilities.

2. Installation and regular update of anti-virus software.

3. Encryption of confidential information on devices that are physically insecure, or not under the University of Toronto's control [see the I+TS Full Disk Encryption website at: http://encrypt.utoronto.ca]

4. Encryption of network communications, such that user credentials and other confidential information are not visible in transit over insecure networks.

5. Protection of networked devices via firewalls.

6. Education of administrators and users as to best practices for protecting data while in storage, use and communication.

7. Physical protection of resources that restricts removal by unauthorized persons.

8. Back up of critical data, with backups tested for readability and protected to the same level as data that is in use.

9. Effective and practiced incident response procedures, including (but not limited to): monitoring of, and response to unauthorized access to systems and data.

10. Disabling un-needed network services.

11. Deletion of 'guest' or non-password protected accounts.

12. Choosing security settings that are more strict than typically insecure default values, and changing default passwords.

For a system to be considered secure, it must have applied the above security practices with a timeliness and effectiveness that reflects the sensitivity of information stored / communicated by the system.

This list of specific practices will be updated as technologies and risk management practices mature; these updates will be communicated to the University of Toronto Information Technology support community.

For guidance on what uses of information and communication technology are considered appropriate, please refer to the policy: "Appropriate use of Information and Communication Technology" (http://www.provost.utoronto.ca/policy/use.htm).