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

CONSISTENT, EFFECTIVE INFORMATION SECURITY

To respond to societal expectations and legislative requirements, the University must create and apply up-to-date information security standards. Should we fail to do so, in the event of a significant release of personal information or compromise of the University's information systems, the result would be a highly visible impact to the University's reputation and stature as a world-class education and research institution.

The need for data classification

There are legislative requirements that require certain controls be applied to select sensitive and personal information. For information with no legislated control requirement, there is still a practical need, informed by public expectations and current practices, to protect data in proportion to the information's sensitivity.

The requirement to protect information

To ensure that information is effectively protected, information must be:

1. Reliably identified by sensitivity, as per current Data Definition guidelines (Appendix 1);

2. Verifiably protected in accordance with location and sensitivity, as per current Data Protection guidelines (Appendix 2);

3. Retained for a duration as defined in the current Data Retention and Disposal guidelines (Appendix 3); and

4. Disposed of as defined in the current Data Retention and Disposal guidelines (Appendix 3).

APPENDIX 1 - DATA DEFINITION GUIDELINES

In discussing access controls for information, information is considered to be either confidential or non-confidential.

Confidential information includes:

1. Any personally identifiable information (PII): name, address, health data, or any other information uniquely associated with an individual.

2. Any data of a financial or legal nature, where disclosure or sharing has not been explicitly authorized.

3. Data associated with access control, such as passwords or door-lock combinations.

4. Information that does not fall into the preceding three categories, but where there is an expectation that the information not be modified, deleted or shared without conscious authorization by the data owner to allow such activity.

All other information is considered non-confidential.

When confidential and non-confidential data are aggregated, the collection as a whole must be considered confidential. Unless designated otherwise, information is considered confidential by default.

APPENDIX 2 - DATA PROTECTION GUIDELINES

Data must be protected from unauthorized access or alteration while the data are in use, in physical or electronic storage, in physical transport or electronic communication, or under administrative access. Access to confidential information must be on a need-to-know basis only; need-to-know requirements must be documented as a requirement of job duties or contractual obligations.

Access and alteration controls must manage the disclosure, deletion, modification or duplication of data. Access and alteration controls must be proportionate to the risk to the University due to unauthorized disclosure, deletion, modification or duplication of data, whether confidential or non-confidential.

Protection of Electronic or Machine-Readable Data

Unless stored on secure, University of Toronto-owned equipment, confidential information (as defined in the Data Definition Guidelines), must have one or more of the following protections applied: be encrypted; have all personally identifiable information removed or obfuscated (anonymized); or be sanitized (have all verifiable information removed or obfuscated). Access to confidential information stored on secure, University of Toronto-owned equipment must be controlled in proportion to the information's sensitivity, and provided on a need-to-know basis.

For a system to be considered secure, it must be managed to a standard equivalent to, or better than Appendix 4 – Security Baseline.

Access controls to change, read or delete non-confidential data are not required beyond those necessary to implement functional or operational requirements.

Protection of Printed Data

The only option to protect confidential data in printed format, is to store it under lock and key. The strength of the lock, and the characteristics of the storage facility (passive fire-resistance, fire alarms, fire suppression systems, break-enter alarms, humidity sensors / controls, etc.) must accomodate the physical characteristics of the print medium and the required retention period.

Non-confidential printed data do not require access or protective controls beyond the physical characteristics of the print medium and the required retention period associated with the data.

APPENDIX 3 - DATA RETENTION AND DISPOSAL GUIDELINES

Data vs. Records

Data, in the context of this guideline, is regarded as information in its broadest sense – symbols or patterns that represent meaning; the terms 'data' and 'information' are used interchangeably in this document. For purposes of risk management, 'data' is considered to be to have distinct needs which may differ from those of a 'record', defined as: "any document containing information, however recorded, whether in manuscript, printed, on film or in electronic form or otherwise". *U. of T. Policy on Access to Information and Protection of Privacy* (1995).

While records are comprised of data, data may not – indeed often does not – represent a record in its entirety, or in its most current or officially-recognized form. Data can created through the process of record creation, modification, transport and storage; these data are often invisible, but not irretrievable, and represent risk if they exist without appropriate access controls. For example, computer systems may create 'temporary' files to assist the process of document creation – a record so created may be deleted at the end of its life, but the 'temporary' data associated with its creation may be retrievably found on the system used to create the record.

Note that storage of data is not restricted to workstations, servers and laptop computers, but includes mobile devices (such as, but not limited to, phones and music players), and office appliances (such as multi-function photocopier / fax / printers). These devices must be considered when developing data retention and disposal practices.

Records Retention

The University's recommendations for how long certain records series should be kept, are set out in more than 700 records retention schedules developed by the University of Toronto Archives and Records Management Services. The retention periods outlined in these schedules should be followed and applied to both departmental files, and to any convenience copies. For more information, please see the University Archives' on-line Retention and Disposition Schedules database [http://archives.library.utoronto.ca/dbtw-wpd/textbase/webschedule/].

Record-Related Data

Data associated with records may be created depending on how a record is stored, used or transported. For reference, such data may occur in, but is not limited to, the following contexts:

1. Metadata: Information that characterizes scheduled records, such as, but not limited to: document name(s), storage location, author(s), reviewers, etc.

2. Temporary Data: Working copies or printed 'draft' documents; application-created copies of files, in whole or in part (i.e. 'temp files'); copies of electronic documents in 'trash' folders on computers, but not yet 'emptied' (i.e. deleted).

3. Residual Data: Data created in the process of using scheduled records, such as carbon-copies, mimeograph originals, film negatives, or 'deleted' files in electronic storage.

4. Cached Data: Data retained for reference - either as in a catalogue of documents, or by an application in order to speed up performance. Cached data may include some or all of the content of a scheduled record, or only metadata, and includes search indexes of both scheduled records and associated metadata.

Access Lifetime

Where data are stored in machine-readable format, equipment and software that can interpret and communicate the data in usable format must be kept in working order for the retention duration of the data. Alternatively, the data must be migrated to new storage media in advance of the end of lifetime for its storage media, or the failure of, or lack of manufacturer support for interpreting technology.

Data Deletion

All data associated with a record must be rendered irrecoverable after its retention duration expires. Data associated with the creation, use and transport of a record should be rendered irrecoverable after data are no longer operationally useful.

Where data are stored in printed format, all documents ideally should be shredded as part of the disposal process. Confidential data must always be shredded as part of the data disposal process.

Where data are stored in electronic / machine-readable format, all storage media should be physically destroyed or 'wiped' (over-written with random data a minimum of 3 times) as part of the disposal process. Devices used to store confidential data must always either be destroyed or 'wiped' (as above) as part of the data disposal process. Technology users should be aware of all locations where data are stored in their environment.

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).