INFORMATION SECURITY BASELINE v 1.0

University of Toronto Faculty of Medicine

A. Base Practices

Certain practices have become de facto requirements to protect the confidentiality, availability, and integrity of data. For a system at the Faculty of Medicine to be considered secure, it must have applied the following security practices with a timeliness and effectiveness that reflects the sensitivity of information stored on / communicated by the system. This is not an exhaustive list; additional practices may be applied to further protect sensitive data (see "B. Protected Data. This document will be reviewed regularly, and updated as technologies change and circumstances dictate.

1. Install vendors' software updates promptly, and install and regularly update anti-virus software, where available.
2. Encrypt electronic personal information outside secure University servers.
3. Authenticate users by UTORauth (UTORid and password).
4. Encrypt user credentials and other confidential information so they are not visible in transit.
5. Where possible, encrypt all data in transit between servers and between servers and clients.
6. Educate all IT staff and users as to the information security best practices relevant to them.
7. Restrict removal of physical resources by unauthorized persons with locks and cages.
8. Report all information security incidents through appropriate channels as quickly as possible.
9. Securely destroy data that is not encrypted before disposing of hardware or media.
10. Whenever possible, disable or block un-needed network services, and select security settings (such as password strength) that are stricter than typically insecure default values.
11. Back up critical data, protect backups to the same level as data that is in use, and regularly test backups for readability.
12. Delete or disable 'guest' or non-password protected accounts, change default passwords for accounts that cannot be disabled, and restrict the use of "admin" or "root" accounts to those processes (such as software installation) that specifically require them.
13. Protect networked devices via firewalls set to deny access by default and to allow access by exception only for documented and approved services, and use firewalls to segregate LANs and keep groups of users separate where possible.
14. Use the OWASP 'Top Ten' list of web application security flaws as a guide to avoiding creating insecure web applications, and do a vulnerability scan before putting them into production.
15. Maintain separate development, testing, and operational/production environments, control access to source code, and ensure that test data is carefully selected and controlled.

These practices have been developed in collaboration with the Information Security and Enterprise Architecture (ISEA) office of ITS, based on their *Information Security Guidelines* document. For guidance on appropriate uses of information and communication technology, see the Provost's policy entitled *Appropriate use of Information and Communication Technology*.

B. Protected Data

'Protected Data' (PD) is data that includes the following types of Confidential information: Personal Information (PI), Personal Health Information (PHI), or Financial Information (FI) that does not belong to the account holder, IT-administrator level access to information solutions / infrastructure, and data with externally mandated protection requirements (see "C. Externally Regulated Data" below). This list may be subject to revision as other sensitive data classes are identified or mandated.

For PD and systems handling PD, the following additional information security conditions apply:

1. Complete an Information Risk and Risk Management (IRRM) assessment questionnaire for review by the Faculty's Information Risk Management Program (IRMP) Committee.
2. Effort must be made to identify and use existing University of Toronto information solutions prior to developing / acquiring a new information solution to store or process PD.
3. Record all data assets and hardware assets that store PD (whether it is encrypted or not) in an asset inventory that is reviewed and updated at least annually to ensure that systems storing PD continue to meet security baseline requirements and are accounted for.
4. Develop an Access Control Policy, based on business and information security requirements, that, at a minimum, identifies the data owner, defines the method(s) of identification and authentication and the rules for authorization, and describes the access provisioning process.
5. Host new in-house PD solutions in a University of Toronto data centre that is protected from unauthorized access, environmental hazards, and power and other utility failures.
6. Authenticate access via a combination of:
    a. UTORauth (using the UTORid/password, and the SAML authentication service), which logs all authentications to the University's incident management service
    b. A second authentication factor that is non-duplicable and is managed either by ITS (specifically the SafeNet eToken service) or by Discovery Commons
7. Undergo 3rd party vulnerability scanning on at least a quarterly basis, and after every major change to the solution, and take appropriate mitigation measures on a timely basis.

Out-sourced information solutions that store or process PD must be subject to, and meet, the same information security requirements that are applied to in-house PD solutions. In addition, information security requirements must be documented and agreed to by the vendor, and regularly reviewed.

C. Externally Regulated Data

Protected Data also encompasses data that may come to the University with external security guidelines or obligations. Such data may include, but is not limited to:

- Credit Card Data
- Legal Data
- Medical Data
- Intellectual Property

These external requirements may compliment or guide the practical implementation of legislation, as determined by professional or other authoritative bodies. In all cases, the more stringent data protection requirements – internal, external, or a combination – must be followed.