Jewish General Hospital
Lady Davis Institute
Information Technology Services

Policy (IT) - Responsible use of IT

The Lady Davis Institute (LDI) Information Technology (IT) resources serve all members of it's institution. Its main mission is to facilitate research in the different fields of research. The LDI IT Services is responsible for ensuring the effective and reliable operation of our systems and protection of our information technology resources. This policy outlines the responsibilities of the LDI IT and its members in the use of IT Resources.

Definitions:

For the purposes of this Policy:

1.1. “Administrative Web Site” means those pages or sites that deal with the administrative aspects of the unit’s roles and responsibilities within the LDI.

1.2. “Authorized User” is a member of the LDI community who is an employee, student, appointee or other individual who has been granted permission, by virtue of the individual’s role and responsibilities, to access certain data or systems that are part of LDI IT Resources.

1.3. “Availability” means the accessibility of LDI IT Resources for their intended use.

1.4. “Broadcast Communications” means e-mail or other electronic communications transmitted through LDI IT Resources to a group, including, but not limited to distribution lists.

1.5. “Confidentiality” means the non-disclosure of Credentials or Data to unauthorized individuals or systems.

1.6. “Confidential Data” means Data that is of a private, proprietary or otherwise sensitive nature, including, but not limited to, Personal Information.

1.7. “Credentials” includes usernames, access codes, account numbers, passwords, PINs, tokens or other authentication which have been assigned to Authorized Users to access LDI IT Resources.

1.9. “Data” means information stored in or transmitted through LDI IT Resources, including documents, files, databases, e-mails and multimedia.

1.10. “Integrity” means protection from modification of Data by unauthorized individuals.

1.11. “IT Guidelines” means the set of the current guidelines or standards related to this policy appearing in the IT Knowledge Base on IT Services portal.

1.12. “IT Services” mean the LDI unit that deliver information technology services on all LDI sites.

1.13. “LDI e-mail address” means an e-mail address issued by IT Services to an Authorized User, according to the official format as defined by IT Services. For example, the LDI e-mail address for its members is usually firstname.middle.lastname@ladydavis.ca

1.14. “LDI IT Resources” means all Data, software, hardware, communications systems, storage systems, networks and devices connected to or making use of the LDI Network, regardless of who administers them.

1.15. “LDI Sponsored Public Web Site” means a web site that is hosted on LDI IT Resources and is accessible by anyone with a web browser and access to the Internet.

1.16. “Non-LDI Use” means use that is not in accordance with section 2.1.

1.17. “Personal Information” means information concerning a natural person that allows the person to be identified as provided for in applicable Canadian and Quebec privacy legislation.

1.18. “Security” means the protection of Data and systems from breaches to or of Availability, Confidentiality or Integrity of LDI IT Resources.

1.19. “System Administrator” means an individual responsible through position description or position responsibilities for establishing and maintaining a computer system or network.

1.20. “LDI Network” means the wired and wireless network for Data, voice and video under the control of IT Services.

2. General guidelines

2.1. Authorized Users shall use LDI IT Resources in an ethical, responsible and lawful manner, in accordance with LDI policies and Quebec laws.

2.2. Authorized Users shall take all reasonable steps to protect the Confidentiality, Integrity, and Availability of LDI IT Resources.

2.3. Authorized Users shall only access LDI IT Resources in accordance with LDI’s policies and procedures. Ability to access LDI IT Resources does

not, by itself, imply authorization to do so.

2.4. Authorized Users shall respect the intellectual property, including but not limited to, trademarks and copyrights, of owners of software and Data stored in or transmitted through LDI IT Resources.

3. Credentials

3.1. Authorized Users shall not share their personal Credentials with other individuals. Where it is essential that an account be shared and delegation is not supported by the application, the Authorized User should contact IT Services for an approval first.

3.2. Authorized Users shall properly identify themselves in applications, services, or connections that use LDI IT Resources. An Authorized User shall not impersonate another person.

4. Security

4.1. Authorized Users shall take the measures necessary to protect the Security of LDI IT Resources and shall comply with LDI policies and procedures concerning data protection and records management.

4.2. Authorized Users shall not use LDI IT Resources for any purpose that puts the institute at risk of compromising Security.

4.3. Authorized Users shall comply with all LDI protocols for reporting threats to Security and shall cooperate with investigations of possible breaches.

4.4. Individuals using LDI-EPI IT Resources in breach of LDI's policies and procedures or in excess of their authority are subject to having their activities monitored and recorded by System Administrators. In the course of monitoring individuals improperly using LDI IT Resources, or in the course of LDI IT Resources maintenance, the activities of Authorized Users could also be monitored.

5. Data

5.1. Subject to section 5.2, Confidential Data shall only be accessed by Authorized Users or by other individuals with a legitimate need to have access who are granted access by an Authorized User. The Confidentiality of the Data accessed shall be preserved and the Data shall be used solely for the purposes for which it was accessed.

5.2. Notwithstanding section 2.3, access to Authorized User Data may be provided to a designated LDI Institute administrator with a legitimate interest in and responsibility for the matter in the following cases: (i) For continued operation of the Institute where the Authorized User whose Data are accessed is unavailable or no longer at the LDI.

(ii) To investigate breaches of LDI policies or regulations where there exist reasonable grounds to believe that a breach has occurred.

(iii) Where permitted by law.

5.3. Before entrusting storage, processing or transmission of Personal Information to an information technology vendor controlled by a company or service outside Quebec, an Authorized User shall consult with LDI IT Services for guidance who will consult with senior administrators as appropriate.

5.4 Research Data cannot leave the LDI network without a written agreement from the main investigator of that study, LDI Information Resources Director or the LDI Director.

6. E-mail and Broadcast Communications

6.1. E-mail services are provided to Authorized Users for the purpose of facilitating effective administrative operations. It is the responsibility of the Authorized user to check his LDI account for any communications. Consult the LDI's Email policies and procedures for a more detailed explanation.

6.2. To ensure that e-mail records are managed according to LDI Data retention policies, all administrative and support staff shall ensure that their LDI e-mail address forwards to an LDI e-mail server. They shall not configure their LDI e-mail to forward to a non-LDI e-mail address, without prior authorization from the IT Services or delegate.

6.3. Authorized Users shall send Broadcast Communications only if the content of the message is related to LDI or administrative functions, and (i) the individual is authorized to send the message by virtue of his or her function or

(ii) the broadcast is sent to a list that individuals have knowingly joined.

6.4. Authorized Users part of administrative units shall send Broadcast Communications in accordance with LDI Guidelines for formats and attachments.

7. Public Web Sites

7.1. An Authorized User who publishes information on a LDI-Sponsored Public Web Site shall ensure that the content conforms to LDI policies and procedures.

7.2. Where LDI sponsors a collaborative web site, such as blogs, wikis or social networks, the site shall conform to IT Guidelines.

7.3. No external or commercial advertising shall appear in any public LDI web site without a prior written approval from IT Services who shall consult the appropriate senior administrator.

7.4. LDI units shall host their Administrative Web Site on the LDI's web publishing system except in the cases of units where functionality requirements cannot be met by the LDI's web publishing system.

7.5. All Administrative Web Sites shall be developed in conformity with the LDI web publishing IT Guidelines, which address Web standards and standards for security, accessibility, and visual identity. In particular, Administrative Web Sites shall be properly identified as associated with and / or belonging to LDI, and they shall provide ease of navigation to and from LDI web sites.

8. Network

8.1. IT Services will use technology to filter any access to the internal network and the internet by any authorized user of LDI IT Resources.

8.2. IT Services shall moderate, filter, limit or block internet traffic, where it exposes the LDI or Authorized Users to threats to Security or where it is necessary to ensure the Confidentiality, Integrity, availability or proper use of LDI IT Resources.

8.3. Authorized Users shall not extend or share the LDI Network with public or other persons beyond what has been authorized by IT Services.

8.4. Authorized Users shall not connect any network devices or systems (including switches, routers, wireless access points, VPNs, and firewalls) to the LDI Network without prior approval of IT Services. Standard exceptions outlined in IT Guidelines shall not require approval.

8.5. Internet use is for academic and research purposes only. All traffic generated from a workstation to the internet is monitored.

8.6 Internet Radio, video streaming, social media, remote access and file downloading that is not for academic or research purposes are not authorized. Internet access is a shared resource between all members of the LDI and must be used for its intentional purpose without abusing it.

8.7 Antivirus and malware software must be running and up to date, in its virus definition, at all time when a workstation is plugged to the network.

9. File Storage & Backup

9.1. The LDI offers to it's members a centralize storage for collaboration purposes. A quota per investigator team is in place. For increase storage space please send a request to IT Services. Consult the LDI's File storage policies and procedures for a more detailed explanation.

9.2. The LDI offers a backup service to all members of the LDI. A quota per member is in place. For increase storage space please send a request to IT Services. Consult the LDI-EPI's Backup service policies and procedures for a more detailed explanation.

10. Compliance

11.1. A violation of the provisions of this policy may constitute a disciplinary offence and, where appropriate, shall be dealt with under the regulations, policies, code or collective agreement to which the Authorized User is subject.

11.2. Any individual who has reasonable cause to believe that there has been a breach of this policy shall report the matter to IT Services who shall notify the appropriate senior administrator.