Jewish General Hospital
Lady Davis Institute
Information Technology Services

# Policy (IT) - General Infrastructure and Security Policy

The LDI (Lady Davis Institute) IT infrastructure will be referred to as The System.

## System Security Overview

### Physical security measures

- All network equipment (switches, firewalls and routers), servers and other networking equipment are stored in locked and secure areas with limited access to authorized personnel only.
- All data centers have an electronic access card system which is limited to authorized personnel only.
- The buildings is under 24/7 video surveillance and regular scheduled round trips by security guards are done.
- All IT equipment, servers, network infrastructure equipment and personal PC's, are kept in locked areas with controlled access.

### Logical measure for access control and privilege management

- All users of the LDI IT System have their own login credentials which are managed by Microsoft Active Directory Services. There are no open or shared credentials.
- All users of the LDI IT System store data and resources on server drives which are controlled by login and user privilege control.
- All user rights and privileges to network data are approved and authorized by the unit supervisor. Records of granted network access are kept and users removed when access is no longer required.
- The data centers uses proven technology to safeguard its data, for example: Cisco ASA firewalls, antivirus, anti-spyware, hard drive encryption, application monitoring, user access tracking, multi-tier backup of all data.
- Unauthorized access to the system will be controlled by authenticating all network access.
- All users are required to sign a confidential agreement that explains the sensitivity of data available to them on the LDI IT System.
- User account password are changed on a regular interval.

### Network security measures

- LDI IT System has a firewall and monitor network packets to ensure that the system is not compromised.
- Firewalls are all set to default deny to prevent intrusion with limited port opening.
- All machines attached to the network are required to have a fully patched operating systems, an up-to-date Anti-Virus protection and a firewall enabled.
- Firewalls set at default deny.
- Any data that needs to be used outside of the LDI IT System has to be stored on encrypted storage devices.

### System Management

- New implementation for a research project will be undertaken by the LDI Service Desk using existing security Policies and SOPs.
- The System is maintained by the LDI IT Multi-Tier Team.
- Server and network security are the main responsibility of LDI IT Team.
- Internal data and local system security is primarily the responsibility of the LDI IT Team.
- The disposal of any computer equipment that has been used to store sensitive data will be done using strict guidelines and SOPs of disposal. All disks will be wiped before being decommissioned.

### Information Security Design

- Paper data of a sensitive nature to be kept in locked cabinets in locked offices with authenticated access to the building and office area.
- Sensitive data are stored on secure servers and access to the data and drive is only permissible to authenticated login only.
- All patient identifiable or nominal data is not authorized to be collected or stored on the LDI IT System. Except for data approved by the JGH Ethic Board.

### The System's authorized users

Only authorized members of the LDI Service Desk who are required to maintain the system.

## Expired Data

When a system or its data has completed its purpose / has become redundant or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data:

- Disks containing data of a sensitive nature, that are no longer required, will be wiped.
- Paper records will be disposed of in a high standard cross paper shredder.

## The System audit

A review of systems architecture, security measures, policies and SOPS are to be undertaken once every 12 months.

## System architecture

All IT systems located within the LDI Datacenters are to be design redundantly to provide resilience and disaster recovery.

- LDI uses clusters of Hypervisor to ensure redundancy in case of a host failure.
- Virtual Machine (VM) are used to house servers that runs critical applications.
- All servers use redundant power supplies connected to redundant Uninterrupted Power Supplies (UPS – Batteries) and backed by generators for long outages.
- All network switches are design with redundancy.
- Cooling systems within the LDI datacenters have redundancy systems.
- Critical services, applications and servers are replicated between our 2 data centers in case of outages.
- In the event of serious disruption or total system failure, business continuity shall be provided by restoring our offsite backup archive following our Disaster Recovery Protocol & SOP.