



<b>Title:</b>	<b>NETWORK AUDIT GUIDELINES</b>
<b>Updated:</b>	March 12, 2012
<b>Audience:</b>	All computer and communication devices owned or operated by the Faculty of Medicine
<b>Purpose:</b>	To ensure the integrity, confidentiality and availability of information resources
<b>Contact:</b>	MedIT

## 1 Purpose

In order to ensure the integrity, confidentiality and availability of information resources, the Faculty of Medicine network staff need to have the authority to conduct a security audit on any system or perform scans on the Faculty of Medicine network. Audits may need to be performed to investigate possible security incidents and to ensure conformance to FOM security policies. Results of audits will remain confidential and are intended solely to provide information to help protect networked computers from non-compliant systems.

## 2 Scope

These guidelines cover all computer and communication devices owned or operated by the Faculty of Medicine. These guidelines also cover any computers and communications devices that are present on FOM premises, but which may not be owned or operated by the Faculty of Medicine.

## 3 Guidelines

When requested, and for the purposes of performing an audit, any access to computer systems needed will be provided to members of the Faculty of Medicine's network staff.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hard copy, etc.) that may be produced, transmitted or stored on FOM equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on FOM networks

## 4 Responsibilities

Faculty of Medicine network staff are authorized to use network scanning, monitoring and audits of computer systems in order to ensure network security and stability. Users should give FOM network staff access to any system requested.

## 5 Compliance

Any staff not providing requested access may have their information systems access restricted or denied.