Title:	**PERIMETER SECURITY GUIDELINES**
Updated:	March 12, 2012
Audience:	All internally connected labs, computer systems, employees and third parties who access the Faculty of Medicine's network
Purpose:	To inform users of our requirements to secure remotely connected systems accessing our internal networks
Contact:	MedIT

1 Purpose

These guidelines are designed to inform users of our requirements to secure remotely connected systems accessing our internal networks. It is in place to ensure confidential information and technologies are not compromised, and that computer systems and data are protected from Internet activities. At the same time efforts will be made to promote ease of access to information between departments and on the Internet.

2 Scope

These guidelines apply to all internally connected labs, computer systems, employees and third parties who access the Faculty of Medicine's network. All existing and future equipment, which fall under the scope of these guidelines, should be configured according to the referenced documents. Stand-alone, unconnected networks are exempt from these guidelines.

3 Guidelines

In order to ensure the confidentiality and integrity of the Faculty of Medicine network, the following equipment and procedures will be put in place. Firewalls maintained by FOM network staff will be utilized for the protection of authorized FOM hosted services, data and computers. All access to the Internet should be routed through the firewalls. Servers and services that will be available on the internal networks should be installed or audited by FOM network staff. Default guidelines of denying all access from the Internet will be adopted with exceptions being made on a case by case basis. Access from trusted remote networks through VPN's will be allowed as long as remote systems are in compliance with the FOM Perimeter Security Guidelines.

4 Responsibilities

1. Research labs, faculty and other groups should assign a primary person responsible for their systems (defined here as a Point of Contact, or POC). Lab owners should maintain up-to-date POC information with FOM network staff. Lab managers or their backup should be available at all times for emergencies, otherwise actions will be taken without their involvement.

2. Lab managers are responsible for the integrity and security of their laboratory computer systems.

3. Lab managers are responsible for the lab's compliance with all Faculty of Medicine security policies. The following are particularly important: Responsible Use Guidelines, Antivirus Guidelines, and physical security.

4. The Faculty of Medicine network staff should maintain a firewall device between the Internet and all internal network equipment. In some cases, this will be a mandatory requirement to secure administrative and sensitive data.

5. UBC IT Services and the Faculty of Medicine network staff reserve the right to monitor and scan network computers and to interrupt connections that impact the internal network negatively or pose a security risk.

6. Any external connections other than through the firewall should be approved by FOM network staff.

7. One computer or networked device may be attached to a single IP address provided to access the FOM network for Internet access. Proxy networks and other methods to share a single network IP is not allowed unless specifically authorized through the FOM IT Support Group.

8. To maintain the security and integrity of both the hospital and the UBC network, no computer or networked device may be connected to both the UBC Network and the hospital clinical network.

9. Wireless networks on Faculty of Medicine administered networks within Hospital clinical and research areas must be authorized through by Faculty of Medicine IT Support Group and be in compliance with security policies with the respective Health Authority.

5 Compliance

Any research staff, faculty, administration staff, students, users and computers found to have violated these guidelines may be denied access to the network.

6 Definitions

DMZ: Demilitarized Zone, special network security zone intended for hosts running difficult to secure services.

Firewall: Security device used to block unsafe network traffic.

Perimeter: Boundary between the FOM network and the University's backbone/Internet.

Service: Any program to which users can connect in order to access FOM related content. These include services such as web, mail, file and print, database and backup.

VPN: Virtual private network, an encrypted, authenticated, trusted connection from an external network to the Faculty of Medicine network.