

| | | |
|-----------------------------------------------|--------------------|-------|
| Subject/Title: INFORMATION SECURITY | POLICY NO. 1438 | Page: |
|-----------------------------------------------|--------------------|-------|

APPENDIX "D"

INFORMATION SECURITY ORGANIZATION

Information Management Steering Committee is responsible to provide guidance for the development and implementation of the Region's Information Security and Privacy policies and processes, and IT Security Standards. Other individuals and groups holding specific responsibility for Information Security and privacy within the Region include:

Access, Security, and Confidentiality Committee (ASCC) is responsible to identify, develop and promote the Region's Information Security and Privacy policies and processes as defined in the Committee's terms of reference.

Information Security Group (ISG) coordinates the Region's responses to Information Security Incidents. This group is responsible to:

- coordinate the implementation of the Region's Information Security policy;
- promote Information, IT, and physical Security policies while providing coordination and technical support;
- assess practices and processes, as needed;
- support training and awareness; and
- oversee an annual Security audit.

Information and Privacy Manager has delegated authority by the CEO, in accordance with the requirements of FOIPP and HIA, to:

- ensure the Region's compliance with HIA and FOIPP;
- establish, monitor and enforce Information Security and Privacy policies and processes for the management of personal and health Information and records in the custody or control of the Region;
- investigate and direct the Region's responses to Information Security Incidents that contravene legal or professional and ethical standards; and
- establish retention procedures and policies for Region Information.

Information Technology (IT) Security Office coordinates IT Security activities throughout the Region, and monitor compliance with and implementation of Information Security and Privacy policies (see IT Resource Security Policy #1487). The IT Security Office is also responsible for the development and publishing of the IT Security Standards.

Vice-Presidents, Executive Directors, and Executive/Medical Directors (or designates) implement Information Security and Privacy policies and processes within their respective portfolios, which includes, but is not limited to:

- ensuring the provision of facilities, equipment, and IT Resources as required by the Region's Information Security and Privacy policies;
- responsibility for ensuring the maintenance and enforcement of appropriate Security for Region Information and IT Resources;
- responding to and reporting on Information Security Incidents within their Departments, and cooperating with investigations; and
- reporting regularly to the ASCC Chair on the implementation of Information Security within their areas.

Directors, Managers, and Supervisors (or designates) initiate responses to Information Security Incidents within their Departments as described in this policy.

Information and Privacy Network consists of representatives from Region Departments who, with assistance from the I&P Office, provide support and advice on Information Security within their individual Departments and perform other Information Security activities as required.

APPENDIX "D" Cont'd

