

# **Information & Information Technology (I&IT) Directive**

**Management Board of Cabinet**

**August 24, 2006**

## **TABLE OF CONTENTS**

<b>PURPOSE</b> .....	<b>1</b>
<b>DEFINITIONS</b> .....	<b>1</b>
<b>APPLICATION AND SCOPE</b> .....	<b>2</b>
<b>PRINCIPLES</b> .....	<b>2</b>
<b>MANDATORY REQUIREMENTS</b> .....	<b>3</b>
GOVERNANCE .....	3
COMMON INFRASTRUCTURE .....	3
COMMON COMPONENTS, APPLICATIONS AND SERVICES .....	3
ASSET MANAGEMENT .....	4
INFORMATION MANAGEMENT .....	4
SECURITY .....	5
ARCHITECTURE AND STANDARDS .....	5
PROJECT MANAGEMENT .....	6
<b>RESPONSIBILITIES</b> .....	<b>7</b>
MANAGEMENT BOARD OF CABINET (MBC) .....	7
MINISTER OF GOVERNMENT SERVICES (MINISTER) .....	7
INFORMATION AND INFORMATION TECHNOLOGY DIRECTIONS COMMITTEE (IITDC) .....	7
INFORMATION AND INFORMATION TECHNOLOGY PROJECT APPROVAL COMMITTEE (ITPAC) ..	7
DEPUTY HEADS (DEPUTY MINISTER OR EQUIVALENT AND AGENCY HEADS) .....	7
CORPORATE CHIEF INFORMATION OFFICER (CCIO).....	8
CLUSTER CHIEF INFORMATION OFFICERS (CIOS) .....	8

## PURPOSE

The purpose of this directive is to establish policy and control parameters for the management of information and information technology in the OPS, and to guide the development and periodic updating of operational policies and related documents.

## DEFINITIONS

In this directive:

“agencies” means agencies (including boards or commissions) as defined in the *Agency Establishment and Accountability Directive*, as amended from time to time, and to which this Directive applies;

“CCIO” means Corporate Chief Information Officer;

“CIO” means cluster Chief Information Officer;

“clusters” means I&IT clusters as defined by the *Information and Information Technology Strategy, 1998*;

“I&IT” means information and information technology;

“information” means ministry and cluster information in all forms, in any medium and at all stages of its lifecycle, including the description of information contents; origins, structure and relationships enabling correct interpretation of information; and including technologies currently in use and future technologies;

“information technology” means the equipment, software, services and processes used to create, store, process, communicate and manage information;

“directive” means this Information and Information Technology (I&IT) Directive, as amended from time to time;

“MBC” means Management Board of Cabinet;

“Minister” means the Minister of Government Services;

“ministry” means a ministry of the Ontario government; and

“OPS” means the Ontario Public Service.

## APPLICATION AND SCOPE

This directive applies to all ministries and clusters, to all agencies utilizing OPS information technology infrastructure or subject to the directive in whole or in part by Memorandum of Understanding, and to all information generated by ministries, clusters and agencies and related technology by which it is processed.

## PRINCIPLES

The management of information and information technology in the OPS is governed by the following principles:

- a) Information and information technology are enterprise assets that are managed strategically, effectively and transparently in the public interest.
- b) Strategic and effective management of information and information technology supports public accountability and the prudent use of public funds.
- c) Public access to government services and information through channels of choice is efficient, timely and responsive and supports customer service expectations.
- d) Information and information technology supports workflow and service delivery through optimized use of technology and data and timely access to information and technology expertise.
- e) Governance ensures alignment between business and I&IT directions both at the enterprise and at cluster level, promotes horizontal approaches that get best value, and enables the integration of I&IT across the OPS to support the government's long-term vision.
- f) Common infrastructure eliminates duplication of assets and resources and increases standardization, maximizing efficiencies and reducing per-unit costs.
- g) Widespread use of common components, applications and services allows business solutions to be implemented more quickly at lower cost.
- h) Alignment of information collection with program objectives and business functions avoids unnecessary information collection and retention, reduces privacy risk, and optimizes information management resources.
- i) The confidentiality, integrity, availability and reliability of information and information systems and resources is ensured and security risks are prudently managed.
- j) Architecture standards and guidelines enhance the value of I&IT investments over time by ensuring that solutions are compatible with the OPS environment.
- k) I&IT projects achieve clear deliverables, add value to the I&IT organization, are completed on time and within budget, and serve a clear business or strategic need.

# **MANDATORY REQUIREMENTS**

## **Governance**

1. Ministries, clusters and agencies must participate as appropriate in and comply with the decisions of cluster and corporate governance bodies.
2. The CCIO must ensure that appropriate governance bodies are established in accordance with corporate governance frameworks, and issue model terms of reference for governance bodies.

## **Common Infrastructure**

3. Infrastructure is defined as the physical hardware and software that supports the flow and processing of information, including physical networks, platforms, wireless devices, networks and access points, cellular telephones, mainframe and desktop computers, servers and data repositories, and operating systems and related software.
4. The CCIO must implement, service and maintain a common infrastructure for the OPS.
5. Ministries and clusters must use common infrastructure implemented by the CCIO unless exempted by the CCIO.
6. Where an interim solution exists or has been adopted which is not part of common infrastructure, the responsible ministry, cluster or agency must migrate to common infrastructure in accordance with a plan approved by the CCIO.

## **Common Components, Applications and Services**

7. Common components and applications are defined as technical components and reusable business applications that have already been developed and tested, are adaptable and scalable, and are often bundled with related services and support.
8. The CCIO must develop, test and promote common components, applications and services as required to support common business needs.
9. Ministries, clusters and agencies must use common components, applications and services if they are available, and not develop new components and applications in competition with available common components and applications.

## **Asset Management**

10. Ministries, clusters and agencies must provide data and information required to the CCIO to support the annual asset management planning cycle, using tools and processes developed for this purpose.
11. Ministries, clusters and agencies must decommission redundant or obsolete applications and report on decommissioning activity through the annual I&IT asset management plan.
12. Where an application is being decommissioned and replaced or the need for a new application is identified, the cluster or agency must first determine whether a common component or application, or a suitable component or application already used within the OPS, is available, and if a common component or application or a suitable component or application already used within the OPS is not available, the cluster or agency must in the first instance consider acquiring a proprietary or open-source application, and develop a custom application only if it is the better cost/benefit alternative.
13. When acquiring proprietary or open-source applications or developing custom applications, ministries, clusters and agencies must apply corporate architecture principles, procedures and standards.
14. Ministries, clusters and agencies must comply with operational policy on lease vs. buy when acquiring IT equipment.
15. When considering open-source applications, Ministries and clusters must evaluate the application with a view to fitness for purpose, value for money, adherence to standards, appropriateness of license, and the risk profile of the solution.
16. The CIO must approve open-source applications for a cluster or ministry and the CCIO must approve any enterprise-wide open-source application in accordance with operational policy.

## **Information Management**

17. Information management is defined as the implementation, supervision and control of explicit and iterative processes and procedures that govern the collection, use, disclosure, retention and disposal of information, including personal information, in possession of a ministry, agency, cluster or program area in accordance with recognized standards and best practices.

Ministries, clusters and agencies must

18. develop, document, apply and periodically review information management plans in accordance with frameworks provided by the CCIO.
19. align information collection with program objectives and business functions.
20. ensure that information, including personal information, can be shared across ministries and program areas as an enterprise resource, providing the sharing of information is in compliance with applicable statutes, law, operational policy and agreements (including

inter-jurisdictional agreements), serves a legitimate program need and informs or enables program analysis, performance measurement, or evaluation.

21. complete a Privacy Impact Assessment (PIA) whenever there is a substantive change in the collection, use, or disclosure of personal information, including the creation or modification of a database containing personal information or its associated application, or where the processing and storage of personal information may be out-sourced to an external service provider.
22. manage rights to intellectual property through appropriate contracts and agreements.

## **Security**

Ministries, clusters and agencies must

23. classify sensitive information in accordance with operational policy, and must approve access to sensitive information.
24. identify security requirements for new programs that must be included in program design.
25. prepare security plans in accordance with operational policy for any program that uses information systems and resources, which must include a Threat/Risk Assessment (TRA).
26. implement security measures to prevent or mitigate, detect and respond to security threats and vulnerabilities to information systems and resources at the program and enterprise levels.
27. train employees in security measures to the extent required by their job function and the nature of the information to which they have access.

## **Architecture and Standards**

28. Enterprise architecture is defined as the overall framework and foundation for I&IT strategy, describing the fundamental organizational structure, logical components, and logical interrelationship of a computer, its operating system, and its related servers and network, and is divided into five major domains: business architecture, information architecture, application architecture, technology architecture, and security architecture.
29. The CCIO must establish architecture standards that include, but are not be limited to, business architecture, standardized data definitions, common data elements and common data exchange language, security, application and technology architectures and how they interlink.
30. Architecture Review Board must review cross-cluster and enterprise-wide projects, common infrastructure projects, projects which have an extensive or unique impact on

the business and technology environment, and any project identified by I&IT Controllership or a cluster CIO.

31. A cluster's architecture review board must review any cluster-specific I&IT project.
32. The CCIO must establish technology standards governing I&IT systems design, application development, and information services and standards, as well as architectural standards and guidelines for procured products and services.

## **Project Management**

Ministries, clusters and agencies must

33. manage I&IT projects in accordance with the methodology contained in the OPS Integrated Project Management Framework and Methodology (herein "Methodology") as amended from time to time.
34. manage any group of projects identified with a particular initiative, strategy, or corporate undertaking as a portfolio in accordance with the OPS Project Portfolio Management (PPM) Framework as amended from time to time, providing that all the projects in a portfolio must still be managed in accordance with the Methodology.
35. employ the common PPM application for reporting on project portfolios, providing that local applications for reporting on project portfolios may be used until decommissioned.
36. approve any project with a four-year projected cost greater than \$1M through a gateway review process incorporating review and decision points at critical project lifecycle transitions, in accordance with operational policy.
37. report on large and complex I&IT projects as defined by the Methodology, with projected expenditure of \$10M or more over four years, through the quarterly major project (and project portfolio) reporting process.

# RESPONSIBILITIES

## **Management Board of Cabinet (MBC)**

In respect of this directive, the responsibilities of MBC include,

- periodic review of this directive to ensure it continues to serve the government's I&IT strategy and vision;
- quarterly review of Major Project Report;
- approval of large I&IT projects costing \$10M or more over a four-year period; and
- review of ministry requests for exemption from any part of this directive.

## **Minister of Government Services (Minister)**

In respect of this directive, the responsibilities of the Minister include,

- establishing, amending, replacing or rescinding operational policies on the management of I&IT, not inconsistent with this directive, setting out more detailed operational requirements for ministries, clusters and agencies;
- periodically reporting to MBC on the making of operational policies, for the purpose of demonstrating prudence and due diligence; and
- periodically making recommendations to MBC on updating this directive.

## **Information and Information Technology Directions Committee (IITDC)**

In respect of this directive, the responsibilities of the IITDC include,

- recommending operational policies to the Minister pertaining to the management of information and information technology.

## **Information and Information Technology Project Approval Committee (ITPAC)**

With respect to this directive, the responsibilities of ITPAC include:

- approving I&IT projects whose projected cost is greater than \$1M and less than \$10M over four years, and recommending projects to MBC whose projected cost is \$10M or greater; and
- escalating approval of projects whose projected cost is greater than \$1M and less than \$10M to MBC as appropriate.

## **Deputy Heads (Deputy Minister Or Equivalent And Agency Heads)**

With respect to this directive, the responsibilities of deputy heads include:

- ensuring ministry compliance with this directive and all operational policies made under the directive;

- ensuring consistency between ministry and corporate strategies, plans and operational policies;
- ensuring single accountable executives are assigned as project sponsors to all I&IT projects launched within the ministry;
- ensuring adequate management of I&IT projects for which the ministry is responsible, in accordance with operational policies, and in the context of portfolio management planning where applicable; and
- participating in I&IT governance bodies and processes as required.

### **Corporate Chief Information Officer (CCIO)**

In respect of this directive, the responsibilities of CCIO include,

- interpreting this directive, issuing interpretations of this directive whenever necessary, and resolving any disputes in relation to the interpretation or application of this directive;
- monitoring compliance with this directive and all operational policies made under this directive;
- supervising the provision and maintenance of common infrastructure and common components, applications and services;
- providing leadership and direction to ministries and clusters on the implementation of security responsibilities and plans;
- proposing an annual I&IT asset management plan to MBC for approval;
- establishing key I&IT processes and governance structures and providing a secretariat function for governance committees, including development of terms of reference or (in the case of cluster and ministry governance bodies) model terms of reference;
- leading the development of operational policies and ensuring corporate compliance with operational policies and this directive; and
- approving enterprise-wide deployment of open-source solutions.

### **Cluster Chief Information Officers (CIOs)**

With respect to this directive, the responsibilities of CIOs include:

- ensuring cluster compliance with this directive and all operational policies made under the directive;
- providing expert leadership and advice to ministries in their clusters on how to utilize technology applications to manage information and data that is consistent with this directive and operational policies;
- providing expert leadership and advice to ministries on how to manage information and data that is consistent with enterprise requirements including privacy and access legislation, operational policies and security standards;
- providing advice and leadership in the planning, development, management and communication of cluster information management practices and plans;
- managing cluster-ministry relationships with the consolidated infrastructure authority and the common components, services and applications program; and
- approving cluster-specific deployment of open-source solutions.