

New Zealand Government Information Systems Policies and Standards

Version 0.8 of 11/05/00 11:26

Background

Following the endorsement by Cabinet of an e-government vision, the State Services Commission, together with the Chief Executives' IM/IT Group, has assigned various projects to government agencies to develop a strategy supporting the vision. This strategy was endorsed by the Chief Executives' forum.

The Ministry of Social Policy (MoSP) was tasked with presenting Social Sector Information Systems (IS) and Data Management Policies and Standards to the rest of government, modifying them to an agreed common standard, and publishing them across government. The task has been split into 2 projects, IS Policies and Standards, and Data Management Policies and Standards.

This document represents the output of Information Systems Policies and Standards project.

Guiding Principles

Common standards and policies to ensure data integrity, efficient data communication and effective return on capital investment are key to e-government. The adoption of common IS Policies and Standards is critical to providing the common 'view', which is a pre-requisite of cost-effective e-government.

The IS Policies and Standards are:

- Based on Open Standards, wherever possible
- Supportive of contestable supply from multiple vendors
- Intended to deliver interconnection between products from diverse vendors
- Able to support a very scalable infrastructure.

They allow:

- Delivery of the lowest cost of ownership while performing to negotiated Service Level Agreements
- Enhancement of business practices with the effective use of Information Systems
- Consistent access to validated management information for formulating policy and measuring operational outcomes

Application

These Policies and Standards are expected to be mandated by Chief Executives delivering components of E-Government. The E-Government context which this document relates to is considered to be one in which citizen data and transactions are delivered to or collected from citizens by one or more Government entities. It also includes the transfer of that data between Government Agencies.

Future Direction

It is anticipated that Government will approve the establishment of a core Government unit to oversee aspects of E-Government such as these Policies and Standards. As that unit and various E-Government projects evolve these Policies and Standards will require growth and modification to reflect the more detailed specification of E-Government. The core principles of an architecture based on open standards and contestable supply should, however, remain valid.

Section 1 – Policies and Standards Maintenance and Administration.

This section defines the policies for the production and maintenance of cross Government IS policies and standards. It also addresses issues of compliance. It is anticipated that these policies and standards are mandatory between all Government entities sharing client and/or citizen information.

Policies and Standards Co-ordinator

The Policies and Standards Co-ordinator will be responsible for the co-ordination and maintenance of cross government Information Systems (IS) standards and policies.

This role is expected to be provided within a central agency which has responsibility for Co-ordinating E-Government. At the time of writing this release of the Policies and Standards that agency has not been defined. Until the role has been established the Information Systems Co-ordinator at Ministry of Social Policy will provide this role but any changes to this document will only result from action initiated at the direction of the Chief Executive's IT forum.

FUTURE DIRECTION

It is anticipated that the Policy and Standards Co-ordinator will convene a working group of E-Government participants to review the performance of the standards and update them as processes and technologies evolve. Such a review should occur annually or as directed by the Chief Executives IT forum.

Co-operative Project Approval

Government Entities participating in co-operative E-Government projects will agree on the project Terms of Reference prior to initiating significant expenditure on the project.

The Government Entity primarily responsible for the project (The Project Owner) will prepare the Terms of Reference and distribute it to other Government Entities participating in E-Government transactions addressed by the project and allow a reasonable period for comment from those other Government Entries. The Terms of Reference should be formally approved by the Chief Executives of participating Government Entities, prior to the release of not more than 20% of the project budget.

Service Delivery

Service Level Agreements must be developed between Chief Executives participating in E-Government transactions.

The Service Level Agreement will include the following:

- Fault escalation procedures
- Required Security
- Network performance
- Required transaction levels, latency and throughput
- Cost apportionment
- Business Continuity
- Compliance with Standards and Policies

It is anticipated that a single E-Government Service Level Agreement will exist between each relevant Government Entity with separate schedules for different classes of transactions.

Policies and Standards Compliance

Chief Executives participating in E-Government will produce a quarterly schedule of their Agencies delivery of E-Government services against the service level agreement.

The Schedule of Performance will be distributed to the other parties to the Service Level Agreements and to the central agency responsible for the monitoring of E-Government. Any issues identified in the Schedule of Performance must be addressed in consultation with other participating Agencies and the plan for resolution of the issue(s) lodged with the monitoring agency.

FUTURE DIRECTION

At the time of preparation of this document a central agency to monitor E-Government had not been established. Until that has been done the State Services Commission will fulfil this role.

Section2 – Information Systems Architecture

This section provides the policies and standards for shared infrastructure, application and network components which are required for the reliable and secure exchange of information between Government entities.

Information Systems Architecture

Information systems components which enable the E-Government vision must conform to these Policies and Standards. Wherever possible such components must also be available from contestable vendors and comply with relevant currently supported IETF standards.

Infrastructure components must support transactions across multiple Government agencies in a secure, reliable and cost effective manner. Ensuring those components are available from and supported by competing vendors will provide a high probability that such systems are able to continue to deliver E-Government in the long term for a reasonable cost.

Internet Engineering Task Force (IETF) standards are currently available across a wide range of vendor products and have proven their ability to deliver efficient service across diverse platforms.

Current IETF standards which are relevant to E-Government are:

- TCP/IP as the network protocol
- SMTP and IMAP for mail transport
- LDAP for Directory services
- HTTP for delivery of client transactions and information

Specific standards to be used for delivering components of E-Government will be agreed between participating agencies and clearly documented in the project Terms of Reference.

FUTURE DIRECTION

Agencies participating in E-Government should continually monitor the development and implementation of emerging standards. However until such standards receive widespread support in the community and are supported by multiple vendors they should not replace any existing standards.

International & NZ IT Standards

Where IT standards or IT industry trends are clear, well established, contestable, and comply with the previous Information Architecture Policy, Government will move to adopt these in a controlled and cost-effective manner

The evolutionary adoption of established standards will be encouraged with the promulgation of Government policies on those standards.

Where IT standards and trends are uncertain, the Government, through the central agency responsible for these standards, will monitor their development and will not take a position on these until a dominant standard or trend emerges.

The rate of adoption will be determined by specific business needs, strategic Government IS policies, and what is most cost effective on each occasion that systems development is considered. If technology, including software, satisfactorily meets current and foreseeable business needs, it should not be replaced or upgraded as long as it remains economically serviceable.

However, when technological advance provides more cost effective alternatives the old technology should be replaced, even if it remains functionally adequate.

Contributing to the economic obsolescence of technology will be the increasing maintenance cost of ageing or superseded technology, which is vulnerable to diminishing supplier support as new product ranges are favoured.

Supplier Independence & System Flexibility

Government entities will move to achieve a high degree of vendor independence and flexibility in IS solution delivery. This will be achieved by choosing hardware and software designed for portability, inter-operability, and inter-connectivity.

There are three main elements which contribute towards the achievement of supplier independence and system flexibility. These are:

- Portability;
- Inter-operability; and
- Inter-connectivity.

Industry standards are rapidly emerging to support each of these aspects.

Government entities will encourage the progressive adoption of software development and package selection standards which support the ability to transport applications from one computer hardware environment to another.

The computer systems architecture will be structured to allow ease of inter-operation between systems thereby ensuring reliable transaction sharing. This may be necessary across quite different hardware and application software (including databases) environments.

The rate of adoption of standards and acquisition of compliant information systems will be determined by the economic life and operational viability of Government entities various IS components.

Future purchases need to ensure systems between Government entities can be easily interconnected. This is an important issue when considering networking connections to other Government agencies and commercial organisations outside of the Department.

The Government is operating in a computing environment subject to rapid technological advances with some uncertainty over the long-term financial viability of even the largest vendors. This makes it essential that the Government 'insures' itself for both change and uncertainty and maintains a vendor neutral position to ensure long term continuity and cost-effectiveness of supply and support.

The amount of available information continues to increase rapidly. Only a portion is available electronically and this problem is compounded by the lack of a common method for accessing this portion. Government entities must increase system inter-operability and inter-connectivity to free up data, within legal limits, and achieve greater benefit from it.

These requirements can be best achieved by the progressive application of policies that ensure both a move to 'open systems' not based on proprietary vendor technologies and a competitive market place for the various suppliers.

Section 3 - Software Development

This section defines policies and standards required to ensure that software development projects intended to deliver E-Government are able to effectively support common infrastructure and provide consistent data and user interfaces.

User Interface to Applications

Government entities will ensure that access to any E-Government application is based on Open Systems standards using WWW (World Wide Web) technology and is capable of full functionality from at least the two most common current vendor implementations of browsers .

Web site design should comply with current best practice for presentation and security and to ensure full accessibility the Web Content Accessibility Guidelines from the World Wide Web Consortium should be followed.

Adherence to current Open Systems and Internet standards will enable integration of Intranet services between Government entities and provide reliable and predictable access to clients and citizens, including those with disabilities.

System Localisation

Government entities will ensure that operating systems and applications are configured to support appropriate and consistent New Zealand Language and environment options.

Specifically, the following local country parameters should be used:

| | |
|--------------|--|
| Date Format: | dd mmm ccyy |
| Time: | Appropriate offset from GMT to also reflect daylight saving. |
| Spelling: | International English |

Government entities must ensure that applications can be effectively configured to reflect New Zealand Date, Time and Spelling formats.

Date Integrity

Government entities must ensure that software is designed and tested in such a way as to mitigate any issues relating to data integrity affected by date issues.

Government entities must ensure that all their IT systems and business processes are audited for potential Year 2000 and related issues

Any new hardware, software and software development introduced to Government entities must be qualified as Year 2000 compliant and interface issues, in particular, must be critically examined in both integration and software development projects.

Section 4 - Network Infrastructure

This section will provide the policies and standards to ensure that data networks used for cross Government communication are able to interconnect efficiently and meet required levels of service and security.

Internet Addressing

Government entities will ensure that a consistent and valid Internet Addressing scheme is implemented. A role to be defined within the State Services Commission will oversee the management of address interfaces between Government entities.

The inappropriate implementation of Internet addressing will prejudice the reliability and efficiency of Government's data communication network.

Security

All Government entities participating in E-Government will have a security policy based on the current release of New Zealand Standard 4444 and shall conduct annual audits based on the current release of New Zealand Standard 6656

Compliance with NZS 4444 will provide the framework of measures required to develop and maintain confidence in E-Government participants to manage their information security risk properly and ensure the confidence of New Zealand Citizens.