

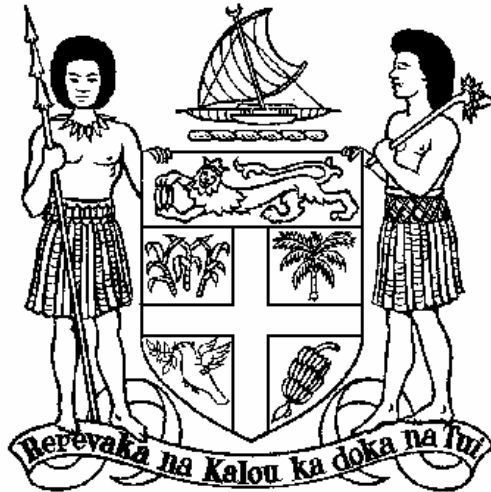
---

---

# THE FIJI GOVERNMENT INFORMATION TECHNOLOGY POLICIES AND PRINCIPLES

---

Version 2.1.0



---

**DOCUMENT APPROVAL**

This document has been reviewed and authorized by the following personnel.

	<b>Writer</b>	<b>Reviewer</b>
<b>Name:</b>		
<b>Position:</b>		
<b>Signature:</b>	_____	_____
<b>Date:</b>	_____	_____

	<b>Quality Assurance</b>	<b>Manager</b>
<b>Name:</b>		
<b>Position:</b>		
<b>Signature:</b>	_____	_____
<b>Date:</b>	_____	_____

**Document Versioning**

**Revision Date:**

**Document Version:**

**Document Path**

T:\Quality Assurance\Documents\Policies, Procedures, Standards\Policies\Fiji  
Govt IT Policy ver1-02-03.doc

---

## TABLE OF CONTENTS

<b>1. INTRODUCTION .....</b>	<b>1-1</b>
1.1. APPROACH .....	1-1
1.2. STRUCTURE OF REPORT .....	1-1
<b>2. EXECUTIVE SUMMARY .....</b>	<b>A-1</b>
<b>3. THE BUSINESS CONTEXT .....</b>	<b>A-2</b>
<b>4. GENERAL INFORMATION TECHNOLOGY POLICIES .....</b>	<b>A-3</b>
4.1. OBJECTIVES OF INFORMATION TECHNOLOGY POLICIES .....	A-3
4.2. CORPORATE DATA POLICIES .....	A-4
4.3. APPLICATIONS POLICIES .....	A-5
4.4. SYSTEM SECURITY ACCESS POLICIES .....	A-6
4.5. COMMUNICATIONS POLICIES .....	A-7
4.6. LOCAL AREA NETWORK POLICIES .....	A-7
4.7. OPERATING SYSTEM POLICY .....	A-8
4.8. DATABASE SYSTEMS POLICY .....	A-9
4.9. MISCELLANEOUS .....	A-9
<b>5. HARDWARE AND SOFTWARE PLATFORMS .....</b>	<b>A-10</b>
5.1. BASELINE .....	A-10
5.1.1. <i>Government Platforms</i> .....	A-10
5.2. TARGET ENVIRONMENT .....	A-10
5.3. POLICIES AND PRINCIPLES .....	A-11
<b>6. COMMUNICATIONS .....</b>	<b>A-12</b>
6.1. BASELINE .....	A-12
6.2. TARGET ENVIRONMENT .....	A-13
6.3. POLICIES AND PRINCIPLES .....	A-13
<b>7. LOCAL AREA NETWORKS .....</b>	<b>A-13</b>
7.1. BASELINE .....	A-13
7.2. TARGET ENVIRONMENT .....	A-13
7.3. POLICIES AND PRINCIPLES .....	A-14
<b>8. APPLICATIONS .....</b>	<b>A-15</b>
8.1. BASELINE .....	A-15
8.2. TARGET ENVIRONMENT .....	A-16
8.3. POLICIES AND PRINCIPLES .....	A-16
8.4. MICROSOFT PATH .....	A-16
8.5. PARTNERSHIP WITH MICROSOFT .....	A-17
<b>9. DATA MANAGEMENT .....</b>	<b>A-17</b>
9.1. BASELINE .....	A-17
9.2. TARGET ENVIRONMENT .....	A-18
9.3. POLICIES AND PRINCIPLES .....	A-19
<b>10. IT ORGANISATION AND MANAGEMENT .....</b>	<b>A-19</b>
10.1. ORGANISATION .....	A-19
10.1.1. <i>Baseline</i> .....	A-19
10.1.2. <i>Target Environment</i> .....	A-19
10.1.3. <i>Policies and Principles</i> .....	A-19
10.2. SKILLS .....	A-20
10.2.1. <i>Baseline</i> .....	A-20

10.2.2.	<i>Target Environment</i> .....	A-20
10.2.3.	<i>Policies and Principles</i> .....	A-20
10.3.	STRATEGIC MANAGEMENT .....	A-20
10.3.1.	<i>Baseline</i> .....	A-20
10.3.2.	<i>Target Environment</i> .....	A-21
10.3.3.	<i>Policies and Principles</i> .....	A-21
10.4.	VENDOR MANAGEMENT .....	A-21
10.4.1.	<i>Baseline</i> .....	A-21
10.4.2.	<i>Target Environment</i> .....	A-22
10.4.3.	<i>Policies and Principles</i> .....	A-22
<b>APPENDIX A FIJI GOVERNMENT PRINCIPLES AND I.T. POLICIES.....</b>		<b>A-24</b>
A.1	HARDWARE AND SOFTWARE PLATFORMS .....	A-25
A.2	COMMUNICATIONS.....	A-25
A.3	LOCAL AREA NETWORKS.....	A-25
A.4	APPLICATIONS .....	A-26
A.5	DATA MANAGEMENT.....	A-26
A.6	IT ORGANISATION AND MANAGEMENT .....	A-27
<b>APPENDIX B INFORMATION TECHNOLOGY STANDARDS.....</b>		<b>B-30</b>
B.1	OPERATING SYSTEMS.....	B-31
B.2	DATABASE MANAGEMENT.....	B-31
B.3	NETWORKING.....	B-31
B.4	HARDWARE AND SOFTWARE STANDARDS .....	B-32
B.4.1	<i>Computers</i> .....	B-32
B.4.2	<i>Fileservers</i> .....	B-34
B.4.3	<i>Printers</i> .....	B-35
B.4.4	<i>Distribution of Large Data-sets</i> .....	B-36
B.4.5	<i>Power Requirements</i> .....	B-36
B.4.6	<i>Modems</i> .....	B-36
B.4.7	<i>Network Card</i> .....	B-37
B.4.8	<i>Switches/Repeaters (Hubs)</i> .....	B-37
B.4.9	<i>Routers</i> .....	B-37
B.4.10	<i>Physical Network</i> .....	B-37
B.4.11	<i>Cabling standards</i> .....	B-38
B.4.12	<i>Software</i> .....	B-39
<b>APPENDIX C COMPUTER SECURITY.....</b>		<b>C-42</b>
C.1	SECURITY AT OPEN OFFICE AREAS .....	C-43
C.2	UNAUTHORIZED ACCESS.....	C-43
C.3	VIRUSES.....	C-43
C.4	ACCESS TO STORAGE MEDIA .....	C-44
C.5	INTERNET CONNECTIONS .....	C-45
C.6	PASSWORDS .....	C-46
C.7	BACK-UPS AND RECOVERIES.....	C-47
C.8	DOCUMENTATION OF ROUTINE ACTIVITIES .....	C-48

## **1. INTRODUCTION**

The Fiji Government requires Information Technology Principles and Policies which are consistent with and which support the long-term strategies of the business.

The objective of this paper was to develop and recommend policies and principles for Information Technology (IT) particularly in the areas of:

- Preferred software and hardware platforms;
- Strategic data management; and
- Strategic communications management.

It is envisaged that the departments of the organisation would then apply these policies and principles in planning and installing their own applications solutions. In particular, they can be utilised in the planning of the rationalisation of future government systems.

### **1.1. Approach**

The paper was written using the framework illustrated below. Tasks undertaken were as follows:

- The business context was briefly visited to confirm and enhance the Fiji Government Information System Group's understanding of the business and environment which IT must support over the next few years
- The current technology baseline was surveyed as a base for future developments
- A broad level vision of the future use of IT in the organisation was developed, and finally
- Principles and policies, which would assist the organisation in moving towards that vision, were developed and documented.

### **1.2. Structure of report**

Following the Executive Summary and review of the business context, the report provides a consolidated form of the IT policies covering all the areas for which they are required. Then follows a more detailed explanation of the policies in terms of the baseline, the proposed target for the future with the recommended policies and principles.

## **2. EXECUTIVE SUMMARY**

The assessment and recommended directions for the facets of Information Technology used to support the business are outlined below.

The Fiji Government currently employs a variety of hardware and software platforms aligned primarily with departments. Benefits could be obtained by moving each department towards a single corporate-wide systems platform in the longer term. These platforms should be (IT) strategic, support the widest range of application operating packages, be based on non-proprietary standards and be non-mainframe in architecture.

The current corporate communications network provides a backbone from which all Fiji IT facilities can be interconnected. This should be progressively expanded, based on modern mainstream technologies, and include overseas requirements as business dictated and should also take advantage of technological advances that offer a demonstrable cost/benefit to the Fiji Government. Use of network solutions not involving the corporate network may be required on a case by case basis, but eventually connectivity to the corporate network should always be considered.

Local Area Networks within the departments vary in nature but should move towards the one systems platform. The Fiji Government should employ a strategy that moves towards the Open System environment, while effectively servicing the system applications to be used.

As expected in government, the Fiji Government will have wide range of System Applications installed. The departments should continue to address application architecture development, prioritising opportunities based on major business initiatives (eg. departmental mergers and corporatisation). Packages should be used wherever possible and external software development organisations used for any custom development addressing areas of high added value for the Fiji Government.

Data Management has, due to the evolutionary development of Fiji Government applications in the past, involved a high level of redundancy and fragmentation.

These are opportunities for the Fiji Government to realise significant benefits by achieving commonality across the departments in some areas, such as financial information, client information and purchasing.

The approach to IT Organisation and management has meant that the IT area and small number of users have largely driven IT development. As the Fiji Government becomes more dependent on IT, both management and users must play a more active role in planning and implementing new technology, with the IT department adopting more a facilitating role with a greater reliance on the business analyst or Departmental coordinators.

It will continue to be difficult for the Fiji Government to retain top quality IT staff due to the lack of a career path for senior IT people, with the importance of controls on IT spending tending to limit the number of highly specialised technical staff. In the future, business people with technical skills, especially in management, need to be encouraged. Opportunities for the outsourcing for more routine tasks must be considered, and specialist skills are provided on a long-term contract basis from external local organisations.

The current IT organisation based on department accountability is appropriate, but the Fiji Government needs to formally define the corporate IT planning process, so that the long term strategic interests of the Central Government are protected and that leverage can be gained from the Fiji Government's planning activities, as globalisation of the organisations increases.

Management of IT vendors is currently often done on a "case by case" basis. Close mutually beneficial relationships with a number of strategic vendors need to be formalised contractually and the vendor management processes used by the rest of the organisation (eg. the use of skilled negotiations, is instigated for IT).

It is recommended that the Fiji Government adopt these statements of direction as company policy.

### **3. THE BUSINESS CONTEXT**

Plans are currently being developed for rationalising and focussing the activities of the government departments on core product streams. Considerable change is envisaged in these departmental units over the next few years in areas such as organisation structure, facility location and function.

The Fiji Government has head quarters in Suva with facilities in the outer islands. The government employs more than 23,000 people at operations throughout Fiji.

The Fiji Government has a significant investment in ITC Services as an IT service bureau. The mission of the I.T.C organisation:

*To meet the needs of Government Departments by providing services of good value and excellent quality.*

The primary goal of the business is:

*To maximise the present value of the projected future cash flows attributable to the Fiji Public (the shareholders)*

The Fiji Governments short term goals are:

- to maintain a 25% return on Investments on plant and internal projects.

Strategies developed to support this objective are:

- high utilisation of assets.
- concentration on specific Public Service areas.
- concentration on key Public Service specialities

The remainder of this report is a list of the recommended policies followed by a more detailed approach looking at the current technology baselines, targets and principles facet of Information Technology.

#### **4. GENERAL INFORMATION TECHNOLOGY POLICIES**

The Fiji Government Policies are outlined in the following paragraphs. These policies are used in determining a corporate information architecture.

Policies are a main consideration to be used by managers and project architects when planning for technology platforms to support business application requirements. Policies carry the decision criteria on risk, growth factors, ownership, security, cost, time frames and implementation priorities.

##### **4.1. Objectives of Information Technology Policies**

The objectives of defining Information Technology Policies are outlined below, they are:

- Definition of Target Architecture - that is business justified and Balances the cost of migration and support against benefits.
- Technology Infrastructure - achieved by combining the required system components to exploit their individual strengths for cost effectiveness and high performance.
- Connectivity simplified - by reducing the number of different environments, standardising protocols, and removing redundancies.
- Common User Interface - by gradual migration, including Consistent presentation, consistent functionality and consistent Control methods.
- Transparent access across system components.
- Transportability of Applications - through use of standard operating system interfaces.
- Component Modularity to allow for enhanced expansion, performance management and availability.
- Meet the immediate technology planning needs - for IT projects currently being planned and implemented by the Fiji Government.

- Simplify Support to minimise the number and range of specialists required.
- Standard Platforms/Applications - (packaged solutions) rather than development and on going support of custom platforms.
- Disaster Management to provide continued delivery of system services in the event of component failure.
- Independence - of particular vendors.

The following sections outline the Corporate Information Technology policies in use by the Fiji Government.

#### **4.2. Corporate Data Policies**

- Data will be considered a valuable corporate asset.
- Data will be captured only once.
- Data will be captured at its source.
- Data will have only one primary store (repository).
- Data stored in the primary store (repository) have a consistent value and structure across the corporation.
- Extracted or summarised data will only be built from data in the primary store (repository).
- Frozen views (either extracted or summarised) of data, created via controlled processes, will be treated as "corporate" data.
- Data will have one owner who authorises its creation, update and access.
- Data will be "defined" by the owner before transformation into an electronic form.
- Data will be held in relational form (RDBMS) in primary store (repository).
- Conceptual data will be "defined" in the data management system.
- Data stored in electronic form will be "defined" in the data management system.
- Data will only be created and updated by controlled business processes.
- Data security will be defined by data (not function).
- All data required for a business function will be capable of integration.

- The data management system will be accessible to all users subject to security controls.
- Copies of data will not exist except for disaster survival purposes.
- Processes, which access, update or create data will be registered against the tables in the RDBMS (database) with the operations they can perform. Object oriented methodologies will be adhered to.
- The location of data will be transparent to applications. It will be located centrally unless it is more cost/effective to place it elsewhere. Before any data is decentralised, consideration must be given to audit trails, security, accountability, responsibility for backup and disaster recovery needs.

### **4.3. Applications Policies**

- For each hardware platform and service category (eg. Batch and Online), one approved application development environment will be defined.
- Applications will use strategic packages supported locally.
- Applications will be developed within the defined Open Systems Interface (OSI) standards.
- Users will have access to applications and data at all times as necessary to support the business needs.
- Users will not need to be conscious of which system applications run on.
- Applications will be located centrally unless it is more cost/effective not to do so.
- The human interface to applications will be consistent across all applications likely to be accessed by any one individual.
- The human interface to applications will be appropriate to the user environment and skill level.
- Applications to support controlled processes will be developed or acquired within an approved development environment.
- The use of applications will be capable of being monitored and controlled.
- Applications will not contain any embedded data.
- Applications will be developed in logical sequence according to corporate data usage requirements (unless overridden by business requirements).

- Established selection criteria will be used to allocate applications to approved application development environments.
- Custom applications and modifications will be contracted out by Tender (minimum 3 quotes from resellers/wholesalers who meet the requirements specified in the tender request).
- Application packages will be selected according to functionality, platform and quality of local support.
- User interfaces will comply with Open Systems Interfaces (OSI) standards.
- The Fiji Government should own application source code if future enhancement to the application is required, otherwise the latest version of the application should be held in a safe deposit facility in a reputable bank.

#### **4.4. System Security Access Policies**

- Each user will have only one personal identification code (user ID). In one work session, users will enter their ID once, regardless of the applications used or the systems on which they run.
- User will be accountable for all actions performed with their user ID. They will be responsible for preventing any other person from using their user ID. Agreements to these conditions will be a prerequisite to granting a user ID.
- Security systems will allow and encourage users to protect their ID code from being used by any other person.
- Security systems will maintain a record of the use of data to satisfy privacy legal requirements and the efficient management of data.
- Actions allowed by clients will be determined by security information associated with their user ID.
- Data access may be managed on either a "need to know" basis (auditors) or by classifications.
- It will not be possible to move copies, extracts or summaries of data from a secure location to a non-secure location.
- Transmitted data will be protected from unauthorized access where necessary.
- Guidelines will be provided for passwords, and periodic password changes will be required.
- Systems department will build a reputation for integrity and discretion.

#### **4.5. Communications Policies**

- Communications Technology to be considered shall be mature or expected to become mature within the next two years.
- Users will be able to use all applications from one workstation or PC regardless of which system the application runs on, subject to security considerations.
- Users will be able to use one remote printer for all applications, regardless of which system the application runs on, subject to security and the requirement for specialised forms.
- Open Systems Interface (OSI) standards will be used for communications between systems platforms.
- All communications technology must support the TCP/IP protocol.
- Integrated voice, video and data communications must be considered in all future plans particularly when installing new Network devices and PABX systems.
- The preferred technology for connection to "outside" facilities will be TCP/IP based.

#### **4.6. Local Area Network Policies**

- Local Area Networks will comply with Open Systems Interface (OSI).
- Extension or development of the network is to be supported by full cost justification.(cost benefit analysis).
- The Fiji Government corporate network architecture and strategy must be documented and included in the Information Technology Policies and Principles.
- To maximise the usability of workstations within its network, the Fiji Government standardizes on Windows NT as the base workstation system and Network Operating System.
- The Network Architecture must be established in such a way as to contain local traffic in discrete LAN configuration, utilising LAN Bridges and Routers to direct traffic between configurations.
- While network versions of software should be employed wherever possible should be distributed, commonly used applications are to be loaded on the individual workstations, to minimise load on the network.
- A corporate wide set of standards should be established for consistent identification of users, workstations and other network objects.

- The network operating system will be supplemented by a standardised anti virus mechanism and a configuration management tool to control both hardware and software configurations. These should be underscored by:
  - standardisation of workstation software for common tasks and office services
  - standardisation of workstation hardware configuration, for memory, display, processor, disc and communications
  - disabling of floppy disc boot capability on all user workstations (where practical).
  - deployment of disk-less systems like Terminal server or Browser hardware devices wherever applicable.
  - adoption of a corporate code of ethics regarding the propagation and use of unlicensed software and the regular conduct of software audits to verify compliance
  - standardisation of system configuration, including directory structures, to simplify management
  - establishment of a consistent and automated backup regime to preserve user data at a central point and assure recoverability in the event of accidental loss.
- Ethernet Bus topology is the standard.
- Network cabling must be CAT 5/7 with RJ45 connectors this applies also for installation of Telephone cabling.
- Fibre-optic cabling implementations particularly for extending LANS in areas where installations are clustered. Network traffic requirements, life-time of the investment and cost of the implementation should be the basis of the consideration to use Fibre-optics
- Office cabling design particularly with regards to furniture layout should be based on 'generally accepted standards' for networking in office areas.

#### **4.7. Operating System Policy**

- The Microsoft Windows XP Professional or greater is the Operating System of choice running on an Intel hardware platform.
- There will be one operating system for each hardware platform.
- Operating systems will incorporate access security.
- Operating systems will conform to Open Systems Interface (OSI) standards.

Note:

Projects affecting the preferred corporate information technology should not be attempted until the expected benefits can justify the development and potential added maintenance costs.

#### **4.8. Database Systems Policy**

- Databases should be of the Relational Database Management System architecture.
- Access to Databases should be through seamless gateways with a capability to do this in real time mode.
- Oracle 9i+ or Microsoft SQL Server 2000+ are the chosen Database platforms.

#### **4.9. Miscellaneous**

Where the required solution cannot be delivered in a timely or cost/effective manner using the preferred corporate technology architecture, the chosen solution must take into account the method and cost of providing interoperability with the corporate architecture via Open System Interface (OSI) standards.

Existing systems that do not fit the corporate architecture will achieve interoperability by using (adapting to) Open System Interface (OSI) standards.

All software and libraries will be protected from access by unauthorized users.

All changes to software and libraries will be by a controlled and managed business process.

One hardware platform will be selected for each technology environment (central processor, personal, LAN WAN, major communications, etc) within each business stream.

For each approved development environment (e.g. 4GL, expert system), one preferred programming technology will be defined.

Technical support will adhere to Open System Interface (OSI) standards as appropriate.

The provision of the best business solution will take precedence over preferred technology environments.

## 5. HARDWARE AND SOFTWARE PLATFORMS

### 5.1. Baseline

The Fiji Government using a variety of platforms including:

#### 5.1.1. Government Platforms

Hosts : Digital Equipment VAX and Alpha  
Operating System : OPEN VMS  
Language : COBOL, Oracle PL/SQL  
The above platform will be removed after December 2005

Host : Intel  
Operating System : MS Windows 2000 Server  
Language : Oracle PL/SQL, MS Visual Basic 6, VS.NET, MS SQL 2000+

Mix of proprietary terminals and PC's running Windows XP, Windows 2000 Professional, Windows NT, Windows 95/98.

All computers bought after January 2003, should have a minimum OS of Windows XP

It is apparent that benefits could be obtained by moving, as opportunities emerge, to those platforms:

- which support the widest range of applicable application packages for the projected future.
- which are strategic (in an IT sense), so that they will remain main stream technologies for the foreseeable future.
- which are based on open rather than propriety standards. To increase inter-connectivity options and allow wider choices of vendor.
- which are based on scalable architectures. To provide better flexibility and scalability in the Fiji Government environment and lower support costs.
- apart from these benefits, a reduced range of platforms will allow better utilisation of specialist Fiji Government (ITC) support staff.

### 5.2. Target Environment

A target of the environment is envisaged at the mid-range level, with the Open Systems environment clearly providing the best option for the Fiji Government at this stage. It is seen to be critical that the number of strategic platforms be reduced

to one in the short (12-24 months) term. The use of the selected environment will provide clear benefits for further rationalisation.

At the workstation level, the Windows environment is clearly standard at this stage. In the future, it is envisaged that MS Windows XP workstations will be strategic. The Fiji Government should resist migration from the NT-Windows environment until further industry standards are established.

It is critical that in the choice of tools for the NT and WINDOWS environments only strategic tools are utilized especially for applications development. The Fiji Government needs to be particularly conservative in this area.

While the Fiji Government has good working relationships with vendors, the continued use of the OPEN VMS and Oracle RDB environment needs to be considered. Although it is generally acknowledged to be a powerful and functional environment, competitive products such as Oracle on NT are clearly market leader and have established themselves as long term strategic vendors, with most application package vendors providing Oracle, MS SQL Server and Sybase based versions of their systems on the NT operating system

The OPEN VMS operating system is losing support from DIGITAL (who will support OPEN VMS for only three more years and is not transparent for corporate data collection purposes. The Fiji Government needs to be particularly careful that it does not end up being a user of the best product, which has only a small number of users.

### **5.3. Policies and Principles**

The Fiji Government should move to standardise on Windows 2000 based environments in the medium term.

Any strategic tools utilised should be in environment, especially for any applications developments NT.

In the NT environment, packages must continue to employ a Relational Database Management System (RDBMS) WHICH IS CAPABLE OF ACCESING DATA FROM OTHER DATABASES through a seamless gateway as supplied by the baseline databases. This access must be in real-time mode. The most commonly used RDBMS are, in approximate order of market share:

- Oracle
- MS SQL Server

In the workstation environment, the WINDOWS environment should be used until Industry standards are established.

Recommended Operating Systems - Strategic Position

- Windows XP or greater.

The NT Operating System is now commonly viewed as a major element of an Open Systems Strategy. Developed initially to provide levels of productivity and application portability than its early contemporaries, NT is finding favour with a wide range of manufacturers of hardware and software as an environment that is also highly portable across hardware platforms.

The current extensive range of available NT solutions is expected to grow rapidly and to continue to converge in the standards sense.

The Fiji Government can be confident that Windows should continue to be the major workstation operating system for the short term.

When industry settles on the next generation of workstation environments, the Fiji Government needs to move on to gain the benefits offered.

#### Recommended Database Management system - Strategic position

- Oracle RDBMS ver. 9i+ or MS SQL Server 2000+

Both are the databases of choice for the Fiji Government, besides being the market leading databases the Fiji government has already made a substantial investment in both database systems. Since making the initial choice, both have moved from being an Enterprise database solution provider to providing a range of database solutions with competitive pricing for the whole range of users.

Users looking for packaged solutions can be assured that either database options will be offered for the majority of solutions that they may wish to purchase, its absence being very much an exception. This is evidence of the Hardware and Software communities' support of this database technology, which means that the Fiji Government can be rest assured that its database solutions will be secure for any foreseeable future.

## **6. COMMUNICATIONS**

### **6.1. Baseline**

The Fiji Government has developed a corporate network architecture based on a Digital Network (supplied by Telecom Fiji) and is progressively moving away from the less effective analogue network links approach as business opportunities dictate. This network will become increasingly important to the Fiji Governments strategy as the need for timely information exchange between government departments and suppliers become more critical.

Currently, the Fiji Government and Government Departments have a requirement for high interactive network traffic, which was not known when the network was

designed. Trials will have to be conducted to determine whether the network will be able to meet this requirement cost effectively.

## **6.2. Target Environment**

Further development of the corporate network to interconnect all facilities of the organisation in Fiji is envisaged. The network will be based on the use of Open Systems (OSI) protocols.

Communications architecture of the future should be based on OSI standards and will be able to support connections to a wide range of carrier technologies

At this stage, however, it is recommended that the Fiji Government should move gradually toward OSI solutions, as business opportunities dictate. It is recognised that specific business requirements may dictate solutions that are not part of the Fiji Government network on a case-by-case basis; but eventual migration back to the corporate network should always be considered in the design stage (and must be cost effective).

There is need for further analysis of the data flow requirements before any specific solutions can be chosen.

General industry trends suggest that fibre-optic networks should be considered to be able to handle future communications involving image transmission.

## **6.3. Policies and Principles**

Any further extension or development of the network is to be supported by full cost justification.(cost benefit analysis).

OSI standards are the preferred direction for any extensions or developments, if justifiable and feasible with hardware and software platforms prevailing at the time.

The Fiji Government corporate network architecture and strategy must be documented and included in the Information Technology Policies and Principles.

## **7. LOCAL AREA NETWORKS**

### **7.1. Baseline**

Current Local Area Networks within the departments vary in architecture, wiring standard and network operating system (NOS), however NT is the de-facto standard and is the most common.

### **7.2. Target Environment**

To facilitate the progressive migration to an Open Systems Environment, the Fiji Government should employ a LAN/WAN strategy that:

- effectively services the application architectures to be employed by the Fiji Government
- is capable of seamless expansion, to accommodate new applications and progressive integration of existing systems.
- employs standard where appropriate
- can be managed from a centralised environment or remotely as required

The LAN market place is currently subject to extensive manoeuvring on the part of Novell and Microsoft, as they seek accreditation with vendors and attempt to position themselves as the dominant player.

- The NT implementation of a LAN Manager, has almost become a standard in Fiji and other parts of the world, having been endorsed by multiple vendors as the Network Operating System for their application products.
- NT offers a high degree of support for the construction of distributed computing networks and is effectively able to support a Wide Area Network.
- Perceived performance constraints applicable to NT in a PC network area able to be overcome by the sheer power of server systems currently available.
- The architecture of the NT environment assures a high degree of operating system portability, which permits it to operate with and to make it readily transportable to the NT Windows group of products

In the mid-term, the Fiji Government should continue with its current dual environment approach. In the longer term, the two environments should be evaluated progressively and a single preferred environment selected.

As stated in regard to communications, the wiring and protocol standards should be reviewed in the context of anticipated future load, especially if image based systems and work-flow management support is anticipated.

As an initial direction, the wiring should be standardised to a common form of cabling and all networks migrated to a single protocol such as TCP/IP.

### **7.3. Policies and Principles**

To maximise the usability of workstations within its network, the Fiji Government should standardise on Windows NT as the base workstation system, as opportunities arise.

The Network Architecture should be established in such a way as to contain local traffic in discrete LAN configuration, utilising LAN Bridges and Routers to direct

traffic between configurations. This architecture will minimise the overall load on the network and preserve performance levels at times of high load.

While network versions of software should be employed wherever possible, commonly used applications should be distributed to and loaded on the individual workstations, to minimise load on the network.

A corporate wide set of standards should be established for consistent identification of users, workstations and other network objects.

The network operating system will be supplemented by a standardised anti virus mechanism, such as Norton's AntiVirus Software and a configuration management tool to control both hardware and software configurations. These should be underscored by:

- standardisation of workstation software for common tasks and office services
- standardisation of workstation hardware configuration, for memory, display, processor, disc and communications
- disabling of floppy disc boot capability on all user workstations (where practical)
- adoption of a corporate code of ethics regarding the propagation and use of unlicensed software and the regular conduct of software audits to very compliance
- standardisation of system configuration, including directory structures, to simplify management
- establishment of a consistent and automated backup regime to preserve user data at a central point and assure recoverability in the event of accidental loss

Note: Application tools: with the proposed systems environment, it would be preferable to use Windows or Web browsers as the standard user interface, unless the given situation dictates otherwise. Development tools should be chosen to maximise the flexibility of the user interface.

## **8. APPLICATIONS**

### **8.1. Baseline**

As expected, by the Fiji Government there is wide diversity in the quality and effectiveness of applications systems installed. Considerable opportunities for benefits are still available from further applications that provide strategic advantage, improve efficiency or reduce application support costs.

The core operational systems continue to serve the Fiji Government effectively, in their current environments, but some cannot readily be expanded to accommodate

extra business activity. Further opportunities will be prioritised by the requirements of major business initiatives (eg. further corporatisation).

## **8.2. Target Environment**

Application architecture development is to be addressed at the business unit level in line with bottom line accountability.

In view of the high cost and risks of custom built system development projects, it is recommended that packages be used whenever possible and that custom built development will only occur to address areas of high added value for the Fiji Government.

The hardware and software platforms recommended will provide the widest choice of low - risk packages, while maintaining uniformity of approach and platforms.

The real cost and risks of custom system development should be managed by a phased approach, with each phase being tendered to fixed price delivery by external software development organisations.

As the corporate business priorities are determined, these will drive the IT planning process to identify further opportunities. A separate report by a Fiji Government Representative and an ITC task force should examine this in more detail.

## **8.3. Policies and Principles**

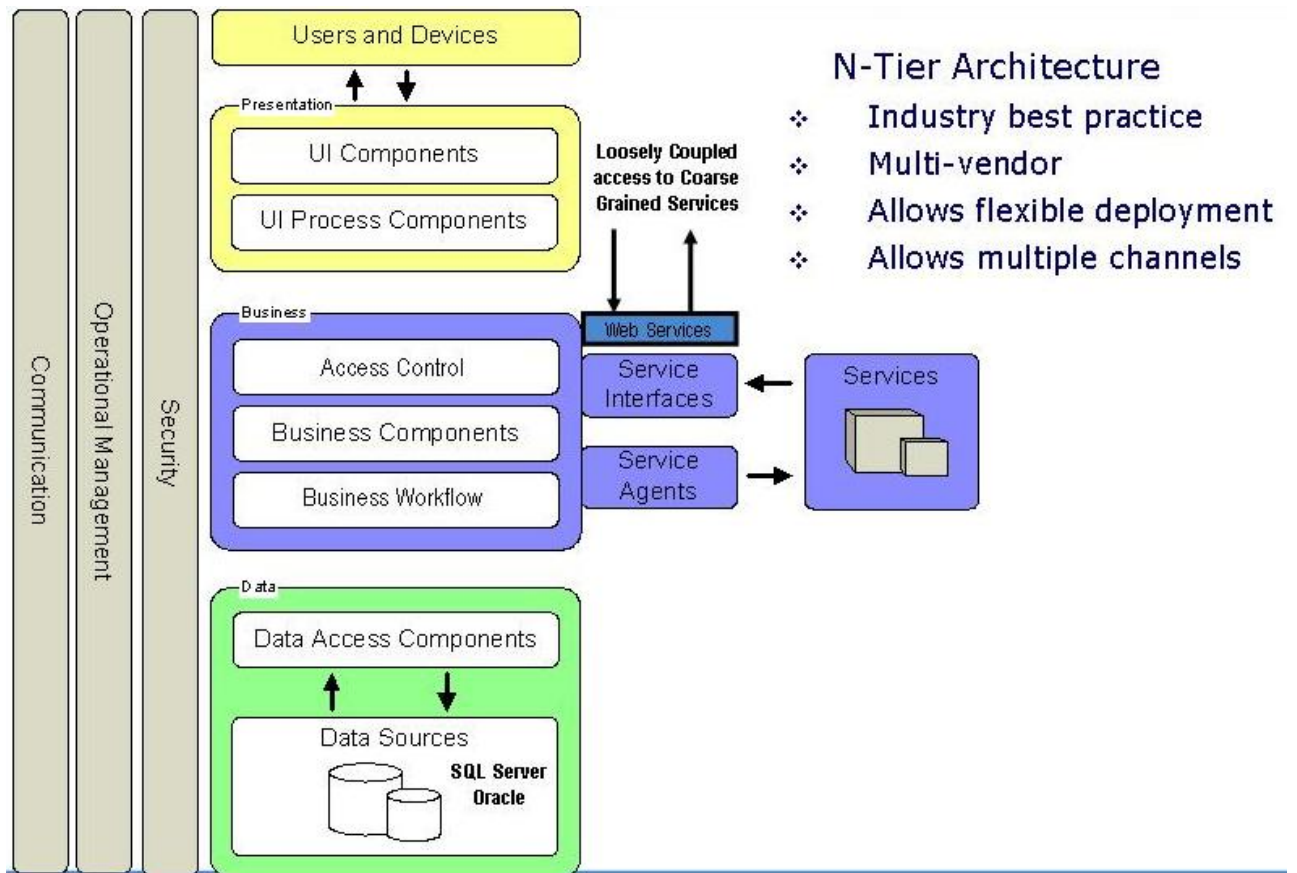
Packages that meet requirements and run on the required platform are to be selected based on the ease of integration with packages already installed.

Custom-built solutions are to be chosen only in areas of high added value.

If a custom built solution is chosen, then the development should be outsourced and performed in a series of fixed-price phases.

## **8.4. Microsoft Path**

The Fiji Government has chosen the Microsoft architectures and framework for applications. All custom built applications have to be designed using the logical architecture below.



## 8.5. Partnership with Microsoft

Vendors seeking to partner with Microsoft can contact the following person:

Dean Dobson

Queensland & northern Territory Consulting Manager

Microsoft Australia

Direct: +61 7 3218 7038

Fax: +61 7 3218 7099

Mobile: +61 (0) 404 827 904

E-mail: [deandob@microsoft.com](mailto:deandob@microsoft.com)

## 9. DATA MANAGEMENT

### 9.1. Baseline

At the moment, organisation data is stored and accessed using a wide range of generally outdated facilities. Due to the evolutionary development of Fiji Government applications in the past, a high level of redundancy and fragmentation

exists. Considerable benefits are envisaged from the adoption of a strategic approach to the enhancement of the Fiji Governments data stores and data management facilities. The first initiative being taken by the Fiji Government is the adoption of databases that allow for communication via the standard baseline providers.

At the moment there is not a perceived advantage from a corporate approach to data management - although a major proportion of clients are common to most departments.

The adoption of data ware housing for data consolidation is and should be the key to data management.

## **9.2. Target Environment**

It is envisaged that each department under direction from the Fiji Government (ITC) would develop a target architecture for data (and also applications) and direct their efforts towards its implementations as opportunities arise.

There may be opportunities in the future for the Fiji Government I.T Policy Unit to realise significant benefits by achieving commonality of information across the divisions, particularly in the areas of:

- financing information (general ledger etc.)
- client information
- purchasing

Managing information for the future will define and target data commonality, such as:

- client account number
- supplier number
- inventory control number
- general ledger number

Commonality of client account numbers should allow single billing and a single sales call (single point ordering), if ever required.

Common General Ledger numbers would allow reports to be generated on Central Government & Departmental basis without need for reworking. The adoption of the MasterPiece General Ledger module is the first step and should be worked on for the provision on communality.

Commonality of supplier number would allow suppliers to be sent one monthly statement rather than two and be paid by one cheque rather than two.

As far as possible the Departments should adopt common data management approaches and standards so that future joint opportunities at the Central Government level can be addressed more easily.

### **9.3. Policies and Principles**

Departments are to develop target data and applications architectures. System development efforts are to be directed towards the implementation of these architectures.

Departments are to cooperate in this area with a view to the adoption of common data management standards and approaches.

## **10. IT ORGANISATION AND MANAGEMENT**

### **10.1. Organisation**

#### **10.1.1. Baseline**

In the past IT development in the Fiji Government has been largely driven from within IT or by a small number of users. As familiarity with the technology improves and this becomes more critical to the overall performance of the organisation, both executives and users will become more involved and more demanding of IT. In the future IT will be expected to provide the same level of risk management and other skills as other areas of the organisation (eg. product development). This will require concerted effort and new approaches to the management of IT. In addition the efforts of IT literate users will need to be aligned with overall business objectives.

#### **10.1.2. Target Environment**

The Fiji Government in future will become dependent on IT and both management and users will play a more active role in planning and implementing new technology.

In the scenario the ITC (as the Governments IT arm) will need to adopt more of a facilitating role with a greater reliance on the business analyst or coordinator.

#### **10.1.3. Policies and Principles**

The Fiji Government should prepare for and facilitate the increasing role of management and users in IT planning development.

## **10.2. Skills**

### **10.2.1. Baseline**

Generally the Fiji Government may find it difficult to retain top quality IT staff mainly because of lack of long term career path for senior IT people who are not interested in a business related career. In addition, it will always be important for the Fiji Government to keep close control on IT spending, so that the availability of highly technically specialised internal staff will be limited. Business people with technical skills need to be encouraged particularly within ITC.

### **10.2.2. Target Environment**

In line with this, the skill set will be oriented towards more business analysts. More outsourcing will be possible for routine needs (eg. data centre management), given the anticipated "commodity" nature of the chosen platforms.

Notwithstanding this, there will be a strong need for the management of system development and information management. Key staff should be encouraged to watch for opportunities for the Fiji Government to improve its practices by the use of IT.

Specialist skills will more frequently be provided through external organisations on a long-term contract basis.

### **10.2.3. Policies and Principles**

The Fiji Government needs to encourage Departmental staff to get more involved and with IT issues, and conversely the current development of the business analyst role within IT departments should be supported.

The Fiji Government should be encouraged to develop an understanding of "IT best practice" in the industry, through their visits to other sites, membership of industry bodies, etc. Combination of these ideas, when combined with an effective approach to IT planning can produce a powerful vision for the organisation.

## **10.3. Strategic Management**

### **10.3.1. Baseline**

The current organisation of IT in the Fiji Government is seen to be less than appropriate. The responsibility for delivery and support at the department level should be in accordance with the "bottom line accountability" philosophy.

However, there is clearly a need for broad guidelines to assist individual areas of the Fiji Government in IT planning so that the long-term strategic interests of the overall organisation are protected.

### **10.3.2. Target Environment**

Further development of the corporate IT planning process is essential to protect the long-term interests of the Fiji Government and to ensure that its competitive position is retained.

It is envisaged that business directions will dictate that more as leverage is gained from the planning and development activities of the Fiji Central Government in the future. The globalisation of world markets and organisations will accelerate this trend.

The Fiji Central Government should be developed to define the corporate IT planning process.

### **10.3.3. Policies and Principles**

Departments should work with ITC services in preparing appraisals for all new IT initiatives. ITC services will help ensure that departments' proposals are aligned to current Fiji Government IT policies and standards. Competitive purchasing practices may also be possible on standard products through ITC services. Appendix D is provided as the working document for such proposals.

Fiji Government IT Policy committee should be the forum where all new IT initiatives over \$10,000 in value (adjusted to the inflation rate) should be tabled for evaluation and approval. The forum will act as a control mechanism for the development of IT in government. ITC services will ensure that all such proposals are put through the appraisal document in Appendix D and are tabled at regular meetings of the forum.

A system inventory will be kept by ITC services to record up to date information on all IT projects that have been undertaken in government. These projects would have been approved by the Fiji Government IT policy committee. Records will also be kept on the progress of new projects and any modifications on current systems.

Ministries and departments should be encouraged to develop IT strategic plans employing people competent with their respective business areas. These should be prepared in conjunction with ITC services particularly on the policy and standards areas to ensure their alignment with the Fiji Governments IT strategy. Strategic plans should then implemented over a period depending on the government priorities in IT investment.

## **10.4. Vendor Management**

### **10.4.1. Baseline**

The Fiji Government currently deals with a variety of IT vendors in a " case by case" manner, and generally has not developed effective long-term relationships with them. This can result in relatively inexperienced negotiations dealing with the highly organised sales/marketing operations of the vendors.

This is in contrast with Fiji Government suppliers, eg. suppliers of IT equipment, where skilled negotiators are used to ensure the best possible deal for the supplier.

#### **10.4.2. Target Environment**

With the preferred platforms outlined for the Fiji Government particularly in the "Open" environment, the government should be well positioned to gain the maximum benefit from a multi-vendor environment.

A number of the technologies recommended as tending to become like "commodities", where specific brands are not important. This is true for both hardware and software and, with the advent of deregulation, communications. HOWEVER, THE TOTAL COST OF IT, WHEN THIRD PARTY SOFTWARE AND TOTAL SUPPORT COSTS ARE INCLUDED, IS EXPECTED TO REMAIN COMMENSURATE WITH CURRENT LEVELS FOR THE FORESEEABLE FUTURE.

The Fiji Government strategic platforms and tools need to be selected with a view to forming close mutually beneficial relationship with the selected vendors. Vendors should be involved in long term planning and committed by means of long-term contractual arrangements. A level of formality in the management of vendor relationships is considered essential.

#### **10.4.3. Policies and Principles**

In the NT environment, any significant (in terms of cost or strategic importance) purchases of hardware should be put to tender. Opportunities to bundle together all required goods and services should be grasped.

Any purchases of standard applications software should be put to tender.

Vendors who provide comprehensive solutions to business problems rather than supplying individual components are preferred.

The solutions may be required to include:

- Implementation
- Training
- Warranty periods
- Maintenance capability (including regular application updates)
- Support capability
- Demonstrated vendor infrastructure for account management

Solutions proposed by vendors should employ only proven technologies to produce innovative solutions for the Fiji Government.

Vendors will provide solutions to business problems, which fit with the strategic directions, platforms and standards should be selected where possible.

Vendors should produce all the appropriate licensing information required for legal ownership on the delivery of software or hardware. Licensing costs should be reflected in costing of any proposals to purchase requests made. Vendors who sell inappropriately licensed solutions will not be considered in future purchases.

Vendors who can demonstrate a long-term initiative/ involvement/commitment to the business factors/applications should be considered and should have two independent credit checks performed.

Vendors should be prepared for penalty payments for non-performance.

All vendors must be ISO 9000 compliant or show proof of current application and documentation of the progress towards accreditation.

**APPENDIX A**  
**FIJI GOVERNMENT**  
**PRINCIPLES AND I.T. POLICIES**

## **A.1 HARDWARE AND SOFTWARE PLATFORMS**

- The Fiji Government should move to standardise on Windows 2000/XP based environments in the short to medium term.
- Any strategic tools utilised should be in the NT environment, especially for any applications development.
- In the NT environment, packages and in-house developments must employ a Relational Database Management System (RDBMS) which is capable of accessing data from other databases. The most commonly used RDBMS are in approximate order of market share:
  - Oracle
  - MS SQL Server

In the Workstation environment, the Windows environment should be used until industry standards are established.

## **A.2 COMMUNICATIONS**

- Any further extension or development of the network is to be supported by full cost justification.
- OSI standards are the preferred direction for any extensions or developments, if justifiable and feasible with the hardware and software platforms prevailing at the time.
- The Fiji Governments corporate network architecture and strategy is to be documented and included in the Information Technology Policies and Principles.

## **A.3 LOCAL AREA NETWORKS**

- To maximise the usability for workstations within its network, Fiji Government should also standardise on Microsoft NT as the base workstation system, as opportunities arise.
- The Network Architecture should be established in such a way as to contain local traffic in discrete LAN configurations, utilising LAN Bridges and Routers to direct traffic between configurations. This architecture will minimise the overall load on the network and preserve performance levels at times of high load.
- While network versions of software should be employed wherever possible, commonly used applications should be distributed to and loaded on the individual workstations, to minimise load on the network.
- The network operating system should be supplemented by a standardised anti virus mechanism, such as Norton's anti-virus software, and a configuration

management tool to control both hardware and software configurations. These will be supported by:-

- standardisation of workstation software for common tasks and office services.
- standardisation of workstation hardware configuration, for memory, display, processor, disc and communications.
- Disabling of floppy disc boot capability on all user workstation (network booting).
- adoption of a corporate code of ethics regarding the propagation and use of unlicensed software and the regular conduct of software audits to verify compliance.
- standardisation of system configuration, including directory structures, to simplify management.
- establishment of a consistent and automated backup regime to preserve user data at a central point and assure recoverability in the event of accidental loss.
- controllable access to server files by directory and file.

Note:

Applications tools: - with the proposed systems environment, it would be preferable to use Windows as the standard user interface, unless the given situation dictates otherwise. NT Developments tools should be chosen to maximise the flexibility of the user interface.

#### **A.4 APPLICATIONS**

- Packages have to be considered in line with custom developments.
- Packages, which meet requirements and run on the required platform, are to be selected based on the ease of integration with packages already installed.
- Custom-built solutions are to be chosen only in areas of high added value.
- If a Custom built solution is chosen, then the development should be outsourced and performed in a series of fixed -price phases.

#### **A.5 DATA MANAGEMENT**

- Business Units are to develop target data and applications architectures. System development efforts are to be directed towards the implementation of these architectures.
- Business units are to cooperate in this area with a view to the adoption of common data management standards and approaches.

## A.6 IT ORGANISATION AND MANAGEMENT

### *Organisation:*

- The Fiji Government should prepare for and facilitate the increasing role of management and users in IT planning and development.

### *Skills:*

- The Fiji Government needs to encourage business staff to get more involved with IT issues, and conversely the current development of the business and government analyst role within the IT department should be supported.
- The Fiji Government executives should be encouraged to develop an understanding of "IT best practice" in the industry, through their visits to other sites, membership of industry bodies, etc. Combination of these ideas, when combined with an effective approach to IT planning can produce a powerful vision for the organisation.

### *Strategic Management:*

- Principles should be developed to define the corporate IT planning process.

### *Vendors Management:*

- In the NT environment, any significant (in terms of cost or strategic importance) purchases of hardware should be put to tender. Opportunities to bundle together all required goods and services should be grasped.
- Any purchases of standard applications software should be put to tender.
- Vendors who provide comprehensive solutions to business problems rather than supplying individual components are preferred.
- The solutions will be required to include:
  - Implementation
  - Training
  - Warranty periods
  - Maintenance capability
  - Support capability
  - Source code if it is felt that the company might not be around in the near future
  - Demonstrated vendor infrastructure for account management

- Solutions proposed by vendors should employ only proven technologies to produce innovative solutions for Fiji Government.
- Ongoing vendors, eg. PC suppliers shall be subject to periodic price and performance reviews.
- Vendors will provide solutions to business problems, which fit with the strategic directions, platforms and standards should be selected where possible.
- Vendors who can demonstrate a long-term initiative/ involvement/commitment to the business factors/applications should be considered and should have two independent credit checks performed.
- Vendors should be prepared for penalty payments for non-performance.
- All vendors must be ISO 9000 compliant or show proof of current application and documentation of the progress towards accreditation.

Principles applied with corporate policies and business application requirements provide the basis for defining standards for the Corporate Information Architecture. The preferred technology platform can then be determined from the alternatives, which best meet corporate needs.

The following principles, provide a basis for developing policies used in supporting project requirements.

The format used here presents these principles in Tiers. In general, Tier 1 values carry most weight and take precedence over Tier 2 and Tier 2 over Tier 3.

#### TIER 1

- Technology Selection - Selection of technology that provides the earliest implementation of the business solution is preferred.
- Technology versus Business Conflicts - Conflicts resulting from the best technology solution for business versus integrated solution economy will favour the best technology solution for the business in the long term.
- Vendor Commitment - Commitment to only those vendors who are willingly provide support to Fiji Government.
- Data Sharing (Managed Data Transparency)- Provide for the controlled sharing of data across business divisions.

#### TIER 2

- Technology Price and Support - Selection of technology within strong competitive lines to provide price and support leverage.

- Technology Selection - Selection of technology, which is proven, in general use with the industry and can be supported by Fiji Government is preferred.
- Security - Technology will be guided by the Fiji Government Security Policy.

### TIER 3

- Technology Expansion - Selection of technology, which allows for controlled expansion and migration.
- Compliance - With open system standards.

## **APPENDIX B**

### **INFORMATION TECHNOLOGY STANDARDS**

## **B.1 OPERATING SYSTEMS**

The Windows 2000 Operating System (the Fiji Government's preferred Operating System) is now commonly viewed as a major element of an Open Systems Strategy. Developed initially to provide levels of productivity and application portability than its early contemporaries, NT is finding favour with a wide range of manufacturers of hardware and software as an environment that is also highly portable across hardware platforms. This high level of portability is largely derived from use of a layered architecture for the core of the system, which separates the basic machine characteristics from all but the innermost core of the system.

The current extensive range of available NT solutions is expected to grow rapidly and to continue to converge in the standards sense, particularly through the increasing use of common tools such as SQL compliant Relational Data Base Management Systems, and a range of high productivity, platform independent CASE tools.

Implementation of other operating systems will require a business case to justify its adoption.

## **B.2 DATABASE MANAGEMENT**

Relational Database Management Systems (RDBMS) have gained commercial acceptance as the chosen database technology. This has become the standard for Fiji Governments database requirements. Oracle RDBMS and MS SQL Server 2000 are the recognised market leaders in terms of market share and technology is the preferred database vendor.

## **B.3 NETWORKING**

The communications architecture of the future should be based on OSI standards and will be able to support connections to a wide range of carrier technologies including:

- High capacity links.
- Metropolitan Area Network capability (ie. between cities).
- Support for TCP/IP protocol.
- LAN-LAN communications at high speed.
- Support for Ethernet Bus Technology.
- Redundant networking.
- Other carriers.

This will allow for information interchange to be tuned to meet the requirements of the business for timeliness, reliability and cost (cost effectiveness).

## **B.4 HARDWARE AND SOFTWARE STANDARDS**

These Hardware and Software purchasing standards are present day 'best specifications' standards. They are prepared with the understanding of the hardware requirements needed to operate effectively the Fiji Governments business. Subsequent updates will be released from ITC services to ensure alignment with changes in the business needs and the market place.

It is possible that Departments may find that changes may be required for specific user requirements. In such cases advice should be sought from ITC Services.

### **B.4.1 Computers**

All computers are to be bought only from:

- Authorised resellers – warranty is guaranteed by them
- Minimum 3 year parts and labour warranty for personal computers and servers
- Minimum 1 year parts and labour warranty for laptops

#### Personal Computer Hardware - Desktop

- Windows 2000/XP
- CPU: Intel, Pentium 4 – 600Mhz+ utilising Intel 815 or later chipset
- Memory: 512MB+ 168pin DIMM (being 1x 64Mb PC-100Mhz compliant piece, leaving slots free to upgrade to at least 128Mb without removing existing DIMMs)
- Hard disk drive: 40.0GB+ - Ultra2 (66Mb/sec) DMA
- PCI Bus Architecture, USB connectivity
- 20x DVD/CR-ROM Drive
- 1.44MB Floppy Disk Dive
- 15" Colour Monitor (1024 x 768 Mhz @ 76hz)
- 4MB+ Video card PCI or (preferably) AGP
- Keyboard (101 extended key board)
- Bus Mouse
- Network card PCI 10/100, RJ45,PXE Compliant, Wake-on-Lan facility on card and PC Motherboard (if network connectivity required)

- Warranty: 5 years, Parts and Labour on site warranty

Only Major brand name machines should be chosen to avoid support problems when maintaining equipment during its lifetime.

Monitor drivers should be available on the Internet.

#### Personal Computers - Notebooks

- CPU Intel, Pentium 4 - 600Mhz+
- Memory : 521MB SDRAM (upgrade to at least 128Mb 256Mb without removing existing DIMMs)
- Hard disk drive: 40.0GB+
- PCI Bus Architecture, USB connectivity
- 1.44MB Floppy Disk Drive
- 12.1" TFT/FRSTN Colour screen
- 2MB+ Video card PCI or (preferably) AGP
- Two Type II PCMCIA Card slots
- PCMCIA 10/100, RJ45, Wake-on-Lan facility on card and Motherboard (if network connectivity required)
- PCMCIA 33.56.46Kbps Voice/Data Modem card (if remote network/computer connectivity or FAX facilities required)
- Availability of “ Docking“Docking Station”. To allow machine to be docked when working in the office.
- Bus Mouse
- Warranty: 3 years, Parts and Labour

#### Personal Computer Software

The following software products represent the minimum requirement:

- Operating System : Windows 2000/XP with latest Service Pack (please refer to ITC for operating system on notebooks)
- Anti-virus software (workstation client version-also available from ITC Services)

Additional software products and licenses may be required depending on the planned configuration of the PC. For example:

- NT Windows 2000 Server CAL (Client Access License), for access to NT Windows 2000 Server file and print services;
- Microsoft SMS License (if PC is connected to government network AND software management required from ITC Services);
- Microsoft Exchange 2000 CAL (for access to government e-mail services)
- Note :Note: A Microsoft “BackOffice” CAL, incorporating the above licenses may be cheaper to purchase than purchasing above licenses separately.

#### **B.4.2 Fileservers**

##### Fileserver Hardware

The following software products represent the minimum requirement (Windows 2000 certification preferred):

- CPU: Intel, Pentium III –800Mhz utilising BX440 or later chipset
- Memory: 256MB+ 168pin DIMM (being 1x 256Mb or 2 x 128Mb PC-100Mhz 133Mhz compliant piece, leaving slots free to upgrade to at least 256Mb without removing existing DIMMs )
- Hard disk drive(s): 18.2-15krpm Ultra / Ultra3-Wide SCSI

Refer to ITC for drive sizing, or depending upon situation - RAID-5 3 x 9.18.20Gb Ultra/32-Wide SCSI, RAID-5 PCI RAID controller card may be required.

- PCI Bus Architecture, USB connectivity
- 15" Colour Monitor (1024 x 768 Mhz @ 76hz)
- 2MB Video card PCI or (preferably) AGP
- CD-ROM
- Network card PCI 10/100, RJ45,PXE Compliant Wake-on-Lan facility on card and PC Motherboard (if network connectivity required)

- Backup: 4mm DAT Tape drive either 4/8 or 12/24Gb capacity. (Refer to ITC for sizing. Please refer to ITC if central backup to ITC can be utilized instead of local backup)
- Power: 30min backup Intelligent UPS (expandability for SNMP option preferred)
- Archive: Write-able CD-ROM or DVD-RAM drive
- Keyboard 101 extended, mouse
- Warranty: 3 years, Parts and Labour,

#### Fileserver Software

- Operating System : Windows 2000 with latest Service Pack
- Anti-virus software (server version)

Two disk options are provided above. The single hard disk drive option for file servers with low availability requirements. The other option is a RAID-5 disk configuration for file servers with high availability requirements, able to endure a disk failure (please refer to ITC for advise upon which configuration would be best suited for your servers requirements).

Apart from the 3-year warranty departments may wish to negotiate special servicing agreements with suppliers before purchasing File servers. This is to ensure a more immediate response to problems. The level of immediacy of response depending on the costs incurred in the loss of the File servers services.

Application servers (Institutional systems, Database systems etc) as opposed to File servers require a detailed understanding of the application before proper configurations can be drawn up. Expert advice should be sought in planning these purchases from ITC.

### **B.4.3 Printers**

Hewlett Packard printers, plotters and scanners are the standard. The model purchased will depend on the requirement, either for portable computing, desktop printing or group printing.

#### Portable printer

HP 720 DeskJet

#### 1 to 4 person printer

HP 2100DN

#### 4 to 12 person printer

HP 4050N

Colour Laser printer

HP 4500N for medium size monthly loads

HP 8500N for large size monthly loads

Flat-bed Scanner

HP 3300C (USB connectivity)

**B.4.4 Distribution of Large Data-sets**

Recordable CD / DVDs prepared on :

Write-Once-Read Many (WORM) or

DVD-Random Access Memory (DVD-RAM)

drives to be the medium for departments that have a requirements to distribute large amounts data. That is data sets greater than 10MB. Each recordable CD should comfortably store up to at least 640MB.

**B.4.5 Power Requirements**

American Power Conversion (APC – [www.apcc.com](http://www.apcc.com) ) are the standard. The model purchased will depend on the systems requirements, refer to ITC for sizing.

Power Protection equipment should be installed with all equipment. Power conditioning plugs and units that protect equipment against power spikes. For more critical equipment an Uninterruptible Power supplies (UPS) with adequate battery lifetime to allow a proper close down of equipment. Any solutions requiring a 'no-downtime' specification should be discussed with ITC Services.

Fileservers are critical equipment and must have a UPS to regulate its power supply. Intelligence should also be purchased to allow a proper unattended shutdown of the Fileserver to be carried out.

**B.4.6 Modems**

- External units
- Voice and Data
- 56.6Kbps +
- Support for Voice over IP and Video H.323
- Rockwell Chipset

- Windows 2000 Ready Certified

External modems are the standard as internal modems are problem prone and significantly degrade the performance of the host machines, also "frozen" internal modems require the powering down of the host machine to reset the modem. Internal PCMCIA card modems of the same specifications are the standard for Notebooks.

NOTE : Modems are prohibited from being attached to the Government network. Attaching modems to the Government network provides an unsecured method of people/organization accessing and/or exploiting confidential government data.

#### **B.4.7 Network Card**

- PCI 10/100, RJ45,PXE Compliant Wake-on-Lan facility on card and PC/Server Motherboard with
- Windows 2000 Ready Certified

#### **B.4.8 Switches/Repeaters (Hubs)**

- UTP port interface (expandability e.g. Support Fibre modules)
- Support for Layer 2/3 switching.
- Support TCP/IP protocol.
- Support Stackable/Hub-mountable configurations
- Support 19" rack-mountable configurations
- Support SNMP / RMON manageable configurations
- Cisco is the Standard

#### **B.4.9 Routers**

CISCO Routers are the standard. Models chosen according to the requirements of each network. Departments are requested to refer to ITC when purchasing network equipment to ensure compatibility with current network standards.

#### **B.4.10 Physical Network**

Ethernet Bus topology is the standard. Building cabling must be CAT 5 with RJ45 connectors. Each run originating from a repeater must be patched to a patch panel. A RJ45 connector should then continue the run coming off the front of the patch panel through a well designed office cabling system to a terminate at a wall-box unit. Machines should then be connected to the wall-box unit via a UTP network card using CAT 5e cable and RJ45 connectors.

Office cabling design particularly with regards to furniture layout should be conducive to accommodating the installation of networking requirements. This will reduce the costs of maintenance and degradation off user's productivity.

Switching hubs are the standard for users requiring the fragmentation of a large LAN in order to reduce congestion in network traffic.

For high capacity network requirements Fibre-optic is the standard. Lifetime of the network must be carefully considered to ensure an appropriate ROI on the implementation. New LAN installations should consider a Fibre-optic backbone.

Established Name brands only are to be purchased to reduce risk of exposure to equipment downtime. Name brands have been listed in particular cases for reasons of security and ease of manageability. Availability of support resources for any equipment on the Internet is also a requirement.

#### **B.4.11 Cabling standards**

These standards are based around the IEEE 802.3 specifications, including 10Base-T, the specification defining 10M-bps Ethernet over UTP wiring.

This document, not only places an onus on the supplier of cabling service, it also has responsibilities for the end-user of the required service. This includes the assigning of secured but accessible and controlled environment, and also the provision of the required power outlets which, preferably, should be filtered.

All cables from hub to workstations should utilise:

- UTP Category 5 or 7 cables (certified).
- All wall plates will only utilise RJ45 connectors as terminating equipment at both ends.
- All patch cables should use color coding:
  - Blue – Workstations / Printers
  - Green –Application/FileServers
  - Red – Network Equipment (Routers etc)
  - Yellow - Voice
- All wire runs, whether it be for voice, video or data will utilise all four pairs of wires in the CAT 5e cable in the single run with a straight through termination.
- All telephone systems will connect directly to an RJ45 patch panel, instead of via a Krone panel.
- All terminating equipment should also be CAT 5/7 certified.

- No single horizontal runs should be more than a hundred meters.
- No runs will be parallel with electrical cables and separated by less than one foot (240V), for loading greater than 240V refer to ITC on a case by case basis. If this is difficult to comply by then they should replace the UTP with STP at no additional cost. This is unless they can provide anti-electromagnetic shield for the duration of the parallel run of less than a foot separation.
- All runs crossing out of doors will have redundancy (double amount required) and will have a metal ducting (if underground) or PVC (if along corridors).
- All wall ports must be within a foot from power outlet.
- All equipment away from the wall will have a specially ducted floor run or ceiling drop right to the actual location so that all equipment will only be one foot or less away from the port laterally. This is not a preferable design as it raises maintenance and aesthetic problems, but may be used if requirements dictate.
- All runs must be separately tested and certified to work and be capable of supporting 100 Mbps with a lifetime warranty.
- All wiring hubs will be located at a secure but accessible room, which can house servers and UPS equipment if the need arises. The room should have air conditioning to enable a controlled environment.
- All runs should be certified at CAT 5/7 \* Fibre compliant, using a CAT 5/7 cable tester (ie using a Fluke cable tester), with print outs certifying this being supplied.

**Leased line terminating equipment should be:**

- Located at private/secure and controlled environment.
- Should be located at a possible location for wiring hubs as mentioned previously.
- Should have power outlets (preferably filtered) within a foot away, located at a place where the horizontal distance to any equipment location is less than a hundred meters away.
- It is required that all new installations be arranged and managed by ITC. This will ensure that the installations are put under the umbrella of the corporate Service Level agreement with benefits that flow from being part of a large Customer account.

#### **B.4.12 Software**

To avoid unnecessary costs due to non-compatibility of information storage formats Fiji Government Software standards have been set. Common software standards also

provide interface common look and feel, common training need and opportunities for corporate purchase agreements.

### Operating Systems

- Microsoft 2000/XP Professional 2000 (with Service Pack 3) or higher
- Microsoft Windows 2000 Server with Service Pack 2 (File Server, Application Server) Linux 8.0 or any other non-Microsoft operating system (for test purposes only – support for these can not be guaranteed by ITC Services)

### Office Suite

- MS Office version 97 / Professional 2000/XP

### Graphical drawing tools

Microsoft Visio Professional ver. 5+

### Project management tool

- Microsoft Project Professional 2000

### Publishing tools

- MS Publisher 98 +2000+
- Adobe PageMaker 6.0

### Databases

- Oracle ver. 8i or over higher (Enterprise, Workgroup)
- MS SQL Server Standard ver.2000 with latest Service Pack (Enterprise, Server)
- MS Access 2002 (Stand-alone desktop applications with 2-4 users only – not for usage on a network)

### E-mail Server

- MS Exchange Server (Enterprise) v2000 SP3 or greater.

(The Government of Fiji Email service is available from ITC. Departments are advised to employ this corporate email system if their requirement is for information exchange with other departments.)

### E-mail Client

- MS Outlook 2000

- MS Outlook Express 5 (Dial-Up users)

#### Browser

- MS Internet Explorer ver.5.5 with latest Service Pack

#### Web Server

- MS Internet Information Server v.45.0 +

#### Compression utility

- WinZip ver. 8.0+

#### Terminal Emulation

- Smart Term / Persona

#### Anti-virus (Desktop, Fileserver)

- Computer Associates Advance AntiVirus Option/InnoculanIT
- Norton's Symantec - Corporate Edition v8.0 recommended client (for all machines AntiVirus (DeskTop) on the network) Norton' AntiVirus (Server)
- Symantec Anti-Virus Corporate Edition 8.0 server (for machines that push updates of definitions to other clients)

#### BackUp (Desktop, Fileserver)

- Microsoft Windows native backup
- Veratis – Please refer to ITC for Pricing
- Computer Associates BrightStor or later (Enterprise, Workgroup, Single-Server versions depending upon requirements.). This is for GOVNET servers housed and maintained by ITC Services. Please refer to ITC for purchasing details, as Enterprise Edition is only sold directly from the manufacturer. The Fiji Government has a account manager from the CA (Auckland) office able to handle inquiries.

**APPENDIX C**

**COMPUTER SECURITY**

## **C.1 SECURITY AT OPEN OFFICE AREAS**

- The Departments information and services, or those of clients shall not be exposed to unauthorised parties.
- Hard copy or soft copy information left unattended in open office environments is vulnerable to unauthorised access, malicious and accidental damage and natural disasters.
- Floppy disks, tape cartridges and other magnetic media shall be stored in filing cabinets when not in use and after working hours. Media containing confidential, critical or sensitive information shall not be left unattended on desks.
- Computer and network hardware or software shall not be taken home by departmental staff without written authorisation by the Departments Security Manager.

## **C.2 UNAUTHORIZED ACCESS**

- All PCs and the information they contain shall be effectively protected against unauthorised access.
- PCs are vulnerable to theft and unauthorised access. They require security to safeguard their contents.
- Portable or laptop computers shall not be left unattended in public places.
- When travelling, portable PCs shall be carried as hand luggage.
- Portable or laptop computers will be locked in the PAO's office when not in use.

## **C.3 VIRUSES**

- The Departments information systems shall be protected from virus attack and other malicious code.
- Computer viruses are self-replicating programs written intentionally to alter the way that a computer operates without the user's permission or knowledge.
- Depending on the motives of the author, a virus may damage programs and data.
- Once a virus has infected a PC, it can rapidly spread to other PCs through the use of floppy disks and via computer networks.
- The objective of this principle is to protect the Departments computer systems from destruction or corruption of information and/or system processes.
- All PC's have been installed with virus protection software to examine all floppy disks upon opening the file and the hard disks in the background.

- Computer viruses when discovered should be deleted or cleaned from the disk. No other option is to be made available.
- All floppy disks coming into a Department will be logged identifying the office of origin with contact name and the contact telephone number and tested for viruses. If a virus is found the floppy disk should be logged out and returned to office of origin with a message attached which states "DISK CONTAINS A VIRUS - PLEASE PRESENT DISK TO ITC. CALL ITC, PC SUPPORT, PHONE 306-005 FOR ASSISTANCE. DO NOT RETURN DISK TO THE DEPARTMENT."
- The Department will then contact ITC providing them with the department, the contact name and the contact phone number of the department with the virus. This information will then be logged along with Department person who made the call and the time the call was made.
- The ITC Help Desk shall be notified whenever a virus is found.
- The Department shall retain copies of the current versions of anti-virus software.
- Anti-virus software shall be installed on all Department File servers and PCs.
- All PCs and file servers shall have anti-virus software operational at all times.
- Only authorised Network administrators shall install and maintain anti-virus software on all network file servers and PC's.
- UNDER NO CIRCUMSTANCE shall anti-virus software be disabled on any file server or PC.
- ITC is responsible for the prompt removal of the virus and investigation of its origin.
- The Department shall ensure that anti-virus software is always up-to-date with the latest virus signatures.
- The Department shall install the updates of the anti-virus software as soon as they are available. The Department administrators will check the availability of the anti-virus updates at LEAST every 14 days and apply any new updates to all systems immediately.
- Failure of Departmental staff to follow the anti-virus procedures will result in disciplinary action by the Head of Department.

#### **C.4 ACCESS TO STORAGE MEDIA**

- Access to storage media shall be controlled in accordance with the security classification of the information stored thereon.

- Information stored on magnetic media needs to be protected in the same manner as if it was printed. This measure will minimise the risk of inadvertent disclosure of confidential information.
- Unauthorised parties should code any media used by Department staff to enable identification by backup software and to prevent unauthorised access.
- All media shall be stored in a secure environment and meet manufacturer's specifications for temperature and humidity.
- All media used on Departmental Information systems to perform backups shall be stored as per the highest security classification allocated to information processed on the system.
- All magnetic media, which needs to be disposed of, shall be destroyed to avoid the potential disclosure of confidential information.
- When media have been authorised transportation, a log shall be kept to confirm that it has safely arrived at its destination address.
- Hard copies of systems documentation shall be physically locked into filing cabinets when not in use.

## **C.5 INTERNET CONNECTIONS**

- All connections to the Internet from a Department shall be implemented under strictly controlled means through the ITC's secure Internet infrastructure.
- The Internet can provide the necessary means for unauthorised parties to access the Departments network, information and systems. To minimise this risk, ITC has implemented a full time, secure Internet connection.
- The download of all software (down loading software is strictly forbidden), can jeopardize the Departments efforts to protect its systems. All downloading must be performed by ITC and transported using the Departments anti-virus checking procedures identified previously.
- It is also important to remember that the reliability and confidentiality of Internet mail messages is not as high as other electronic communications methods. It is strictly forbidden to send confidential mail on the Internet.
- Any staff member requiring full Internet access (not including Internet mail) from their allocated PC shall obtain a formal authorisation from the Department Security Manager.
- Internet services shall be accessed only through the ITC Internet connection.

- Access to personal Internet accounts from Department equipment and Internet service is prohibited.
- No personal Internet software shall be installed on any of the Departments PCs.
- No copyright material shall be downloaded illegally from the Internet, or utilised in breach of its license agreement.
- The Fiji Governments Internet and network resources shall not be used to access for transfer any material containing:
  - -Derogatory remarks based on race, religion, gender, physical disability or sexual preference.
  - -Images or references that may be considered to be offensive or in breach of any law or regulation.
- Application software shall not be downloaded from the Internet, except by ITC staff. Any request for the implementation of non-standard Internet software, such as some type of browser enhancement software, shall be presented to the Department Security, who will liaise with ITC to assess the viability of the request.
- Before sending or requesting a client to send urgent, sensitive or confidential messages via the Internet, preference shall be given to alternative, more appropriate and reliable methods.

## **C.6 PASSWORDS**

- All care shall be taken to ensure that, under any circumstance Department user access passwords are not disclosed to parties other than the intended user.
- Passwords shall:
  - -Not be obvious.
  - -Consist of a mixture of upper and lower case alphabetic and numeric characters, at least six characters long.
  - -Be kept confidential at all times.
  - -Not shared with any other user or party.
- Passwords shall be memorised and shall not be written down. Exception can be accepted for systems id's, where those passwords are kept in an offsite storage vault.
- Passwords shall not be included in any automated or batch process, including macros and scripts.

- Passwords shall be a minimum of eight characters long.
- System files holding passwords, or other authentication codes, shall be protected against unauthorised access by the use of encryption and/or security software.
- All passwords, or other authentication codes, transmitted across the network shall be encrypted.
- The Department shall utilise passwords as a key method for authentication of users. Disclosure of passwords, or other authentication codes, can result in modification, disclosure and destruction of information belonging to the Department.

## **C.7 BACK-UPS AND RECOVERIES**

- All systems software, application software, data and documentation shall be backed-up regularly to enable the system to be recovered with minimal data loss when required and without the loss of integrity.
- An effective backup strategy minimises the potential impact of the loss of data and enables a return to normal operations as soon as practicable.
- Each computer system must be backed up on a regular basis. Backup cycles shall be related to the frequency with which data and software is changed and shall include, as a minimum:
  - -incremental daily backups of all data considered to be critical or important;
  - -incremental weekly backups for all other data; and
  - -monthly backup of all system, application, and data.
- Responsibility for the establishment of appropriate backup cycles rests with ITC.
- The Departments shall liaise with ITC to ensure that implemented backup cycles meet the Departments requirements.
- A cycle of backup tapes shall be used for all backups with at least one copy in each cycle stored in an off-site vault. The off-site vault shall:
  - -be located on a building sufficiently distant from the building where the computer system is located;
  - -provide restricted access to authorised personnel only; and
  - -provide adequate protection against fire, flood and physical disasters.
- No backup tapes or cartridges shall ever be taken home by any Department staff member.

- In addition to regular backup cycles, a system backup shall be performed before and after major changes to the operating system, network configuration, system software, or applications, at the discretion of the Department Administrator.
- Backup tapes are to be held in a location that provides adequate physical security to limit access to authorised personnel.
- A cycle of backup tapes shall be retained of all information required to meet statutory obligations. These backups should be created at least annually and shall be stored off-site.
- In situations where backup copies are not frequently restored, a cycle of regular tests shall be implemented to verify that systems and data can be recovered from the backups produced.

## **C.8 DOCUMENTATION OF ROUTINE ACTIVITIES**

- Routine activities shall be formally documented and followed.
- Procedures for data backup, event logging and environment monitoring are necessary to ensure the integrity and availability of services.
- Backup of systems and data shall be performed daily and stored offsite at a secure location to enable recovery from a disaster.
- The Department shall keep a log of all tape cartridges utilised for backup purpose. This log shall include the:
  - -Cartridge label;
  - -Type of backup performed full, incremental, weekly, monthly or daily;
  - -Date of the backup; and
  - -Date taken to offsite vault.
- Backup data located at offsite storage areas shall receive physical environmental protection at least equal to that which it would receive at the main site or computer room.
- Operations managers shall maintain a log of all work carried out by third parties, and those, which have direct implication on systems availability.
- Environmental controls shall be properly monitored to identify adverse conditions and enable prompt corrective action. This should apply, at a minimum, to:
  - Temperature

- Humidity
- Power supply quality
- Department Staff shall be responsible for the backup of all information stored on their individual PCs' hard disk drive.
- In situations where storage requirements exceed available capacity, information may be archived, at the discretion of the Head of Department.