Government of Belize

Electronic Government Policy

2007 - 2011

Office of Governance

April, 2007

TABLE OF CONTENTS

Executive Summary

Electronic government aims to enhance access to and delivery of government services to benefit citizens. It also seeks to strengthen government's drive toward effective governance and increased transparency to better manage a country's social and economic resources for development. The attainment of "a high tech Belize", as a means of helping people bypass some traditional barriers to development, has been articulated as a specific goal by the political directorate.

Utilizing an evidenced-based policy formulation approach, data was collected and analyzed with respect to ongoing and planned ICT initiatives in the Public Sector. The analysis indicated several key lessons learnt and enabled the preparation of a SWOT analysis on Public Sector ICT and E-Government. The overall finding was that the Government of Belize has embarked on a wide range of ICT related projects over the last decade. Computer technology now plays an increasingly significant role at the operational level of all government Ministries and Departments.

Given the present level of adoption and use of computer technology, the implementation of this E-Government Policy will augur well for the further advancement of the public sector modernization agenda. The objectives of the E-Government Policy will be pursued over the short term (0-2 years), medium term (0-5 years, and long term (0-15 years), in the context of the following vision: the use of information and communication technology (ICT) by the Public Service of Belize to improve the efficiency and effectiveness of service delivery using modern and standardized Electronic Government practices and processes.

This Policy will seek to promote the adoption of the following ISO standards as national standards: ISO 15489 - Information and Documentation: Records Management; ISO 17799 - Information Security Management; ISO 18028 - IT Network Security; ISO 18044 - Information Security Incident Management; and ISO 12207 - Software Life Cycle Processes. Standards for acceptable use, which define the appropriate use and behavior with respect to information and technology resources in the public sector, including copyrighted material, network security, hacking attempts, data, hardware, software and email are also outlined in this Policy.

Three critical components of the enabling environment for the successful implementation of the Policy are addressed: legislative and regulatory framework, institutional framework and human resource development and capacity building. Policy statements with respect to Government to Government (G2G), Government to Business (G2B) and Government to Citizen (G2C) are also outlined.

1. Introduction

1.1 What is E-Government?

Definitions of e-government range from "the use of information technology to free movement of information to overcome the physical bounds of traditional paper and physical based systems" to "the use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees.[1]" The common theme behind these definitions is that e-government involves the automation or computerization of existing paper-based procedures that will prompt new styles of leadership, new ways of debating and deciding strategies, new ways of transacting business, new ways of listening to citizens and communities, and new ways of organizing and delivering information[2].

Ultimately, e-government aims to enhance access to and delivery of government services to benefit citizens. It also seeks to strengthen government's drive toward effective governance and increased transparency to better manage a country's social and economic resources for development.

1.2 Political Context

The 2003 manifesto of the People's United Party of Belize promised "a high tech Belize" as a means of helping people bypass some traditional barriers to development, assuring, that the computer will become more commonplace in homes, at school and in the workplace. To achieve this, competition in the telecommunications market would be encouraged in order to lower rates, ensure wide community access to telephone. Some of the commitments made were to: restructure educational institutions to provide ICT skill development and prepare professionals able to maximize ICT use for development; provide opportunities for the existing workforce to retrain to meet the new ICT, provide the legislative and regulatory framework for effective licensing of new technologies; establish, with the support of the relevant international

---

[1] Deloitte and Touche, (2003) "At the Dawn of e-Government: The Citizen as Customer." http://www.publicnet.co.uk/publicnet/fe000620.htm.

[2] Rogers W'O Okot-Uma, "Electronic Governance: Re-inventing Good Governance." Commonwealth Secretariat, London. http://www1.worldbank.org/publicsector/egov/Okot-Uma.pdf

organizations, a National ICT Advisory Body to recommend strategies for a National ICT Policy and to monitor developments in the field; apply ICT in particular to the health and education services.

1.3 Telecommunications Market Overview

Belize was among the first Latin American countries to privatise its national telecom company in 1988. The incumbent, Belize Telecommunications Ltd (BTL), was given a fifteen (15) year monopoly concession until the end of 2002 for all fixed-line and mobile phone services. International Telecommunications (Intelco) became BTL's first competitor in October 2003, but ceased operations by November 2005. SpeedNet Communications (SpeedNet), began to build a CDMA2000 1X network in September 2004. SpeedNet and other organizations now offer Internet access, wireless broadband and various corporate services as well as mobile telephony at competitive rates to BTL.

In his study on telecommunications in Belize, Samuels (2000), argues that the country's low levels of teledensity limited the country's ability to adopt a wide range of telecommunications services, such as the Internet and electronic commerce. It is argued that one of the reasons for this low teledensity is Belize Telecommunications Limited's (BTL) status as the exclusive provider of national and international telecommunications in Belize since 1988. As part of its monopoly license with the Government of Belize, which expired in January 2002, it was expected to "provide ubiquitous service without prejudice, especially to the rural areas, in terms of the quality of services provided, the type of services provided, and the cost of services provided" (Samuels, 2000).

There has been a tremendous increase in the rate of growth in cellular/mobile phone usage, as well as moderate increases in the internet segment of the telecommunications market in Belize. Data from one of the telecommunications providers indicate connections in the range of 31,000 wireless, 6,700 internet users and 120,000 mobile.[3]

[3] www.btl.net/btl-facts

2. Vision Statement

The vision statement was crafted on the principle of reflecting a demand-driven, development-focused description of a future state of affairs, i.e. subsequent to the successful implementation of the provisions and initiatives outlined in this E-Government Policy:

The use of information and communication technology (ICT) by
the Public Service of Belize to improve
the efficiency and effectiveness of service delivery using
modern and standardized Electronic Government practices and processes.

3. Objectives

3.1 Short term (0 - 24 months)

- Use of ICT to enhance levels of user/citizen trust and confidence by providing convenient access to Government services that are responsive to client needs.
- More effective management of records: data and information in the Public Service.
- Enhance capacity and sustainable use of ICT.

3.2 Medium Term (0 - 5 years)

- The use of ICT as an enabler to the attainment of the MDGs, and in particular: improvement of primary education; gender equality and empowerment of women; reduction of child mortality; improvement of maternal health and to develop a Global Partnership for Development.
- More effective management of knowledge in the Public Service.
- Use of ICT as a tool for engagement of citizens in governance.

3.3 Long Term (0 - 15 years)

- The use of ICT as an enabler to the National Strategy for poverty alleviation (MDG-Goal 1: eradication of extreme hunger and poverty)
- Use of ICT as a mechanism for the meaningful participation of citizens in governance

4. Status Report: ICT in Public Administration

4.1 Background of Public Sector ICT Initiatives

Data was collected and analyzed with respect to ongoing and planned ICT initiatives in the Public Sector. The overall finding was that the Government of Belize has embarked on a wide range of ICT related projects over the last decade. Computer technology now plays an increasingly significant role at the operational level of all government Ministries and Departments.

The introduction and use of ICT in the public service, however has been limited, to some extent, by a lack of coordination and integration in the planning and implementation of these initiatives. This is due largely to the absence of a Policy and Strategic framework which would provide the requisite direction and guidelines for the adoption and utilization of ICT resources in the Public Sector. Given the present level of adoption and use of computer technology, the implementation of this E-Government Policy will augur well for the further advancement of the public sector modernization agenda.

4.2 Lessons Learnt

Some of the key lessons learnt with respect to public sector ICT initiatives in Belize are presented in Table 1 below:

Summary: Lessons Learnt

1. Software licenses need to be regularized
2. Further training to be provided for IT personnel, users and senior management
3. Internet/Data segment of the telecommunications liberalization process should accelerated
4. Continue to engage Banking and other Sectors to facilitate e-transactions
5. Institutional framework for Public Sector IT to be strengthened
6. Review IT job classification to be consistent with other professional streams in the Public Service
7. Open source should be explored as alternative to proprietary software
8. Consistent involvement and participation of End Users in the systems analysis, design and implementation processes
9. Increased financing of public sector IT required
10. Network security to be improved
11. Websites and back-end databases to be further enhanced
12. Public Sector Systems should be better integrated
13. Legislative and Regulatory dimensions to be addressed

4.3 SWOT Analysis

The SWOT analysis presented below is the result of deliberations of the eGe Taskforce, which also entailed a review of the SWOT analysis performed with respect to one of the Key Results Areas (KRAs) for the Office of Governance Strategic Plan: 2006 - 2008:

Table 1: SWOT: ICT and E-Government

Strengths	**Weaknesses**
• Significant amount of content • Established ICT/Electronic Government Unit • Wide Area Network deployed across the Public Sector • Training Facilities available • Trained staff • High level of computerization in Ministries • Support from International partners • Computer equipment available • Existing technology services with private sector entities • Access to Short-term Capacity Building and Training for Public Officers • Use of Open Source Software in a number of Ministries	• Need for integration of infrastructure. • Training for sustainable use of ICT in the Public Sector to be increased • National Accreditation and recognition of training offered in the Public Sector is limited • Underutilization of computer equipment • Legislative framework requires further development • Availability and quality of information is deficient • Limited appreciation of information for decision making and control • Levels of Computer and Information literacy can be improved • Some individuals with responsibility for IT functions are not adequately trained • Deployment and utilization of IT related personnel needs to be streamlined • Systems analysis and design processes to be strengthened
Opportunities	**Threats**
• Emerging Information based society • Awareness of e-Government • Improved service delivery • Maximise the utilization of existing resources • Support from international and regional partners • Reduced operating costs • Public-Private Sector collaboration	• Global environment: security concerns • Retention of trained persons due to inadequate compensation packages and career progression options • Financial sustainability of ICT initiatives • Rapid rate of change in technological and global business and economic environment

5. Standards

Standards are critical for providing the means of rationalizing markets and facilitating international trade. The WTO's Agreement on Technical Barriers to Trade (TBT) includes the "Code of Good Practice for the Preparation, Adoption and Application of Standards" which recognizes the important contribution that International Standards can make to improving efficiency of production and facilitating international trade.

Acknowledgement of the strategic role of International Standards for development and trade, as well as operationalizing the global Information Society was one of the achievements of the first phase of the World Summit on the Information Society (WSIS) held in Geneva in December, 2003. The resulting summit Declaration of Principles recognizes that international standardization is one of the key enablers for the development of a Global information Society:

> Standardization is one of the essential building blocks of the Information Society. There should be particular emphasis on the development and adoption of International Standards. The development and use of open, interoperable, non-discriminatory and demand-driven standards that take into account needs of users and consumers is a basic element for the development and greater diffusion of ICTs and more affordable access to them, particularly in developing countries[4].

Consequently, this Policy will seek to promote the adoption of international standards set by recognized bodies as national standards. In the Caribbean Community, it has been suggested that international standards can serve as instruments that enable the development of harmonized, stable and globally recognized framework of technologies, best practice and agreements to support the overall growth of the CSME[5]. In addition, it is clear that "the adoption of ICT standards, rules and codes of practice that are shared and adopted on a global scale will help to guarantee security, to develop consumer confidence and protection" (Rhone, 2005). In this regard, the following International Standards are proposed for adoption and implementation:

[4] WSIS (2003). Building the Information Society: A Global Challenge in the New Millennium. Item 44, Section 6.

[5] Rhone, C. (2005). "Standards: Central to the Growth of the ICT Sector in the CSME." CARICOM Perspective, No. 72, Vol. 2, July 2005.

5.1 Data and Information Management

With records (representing Data, Information and Knowledge) constituting one of the most important aspects of public sector operations, the way they are created, managed and stored, has a phenomenal effect on our organizational success and on the smooth-running of operations. Badly managed records and information impact across an organization on a number of levels, and whilst periodic assessment of data storage might be quite challenging and time consuming, its benefits can contribute significantly with the role of information management in the Public Sector modernization process.

One of the aims of ISO Data and Information Management standard (ISO 15489 - Information and Documentation: Records Management) is to help organizations recognize the importance of their business records (whether electronic data, forms, images or documents) and promote best practice within records management. The benefits of a full ISO 15489 implementation are wide-reaching. An organization's records and information management and recordkeeping processes will become more effective, giving rise to efficiency savings, reduced costs and increased service delivery.

Organizations achieving ISO 15489 compliance will be able to demonstrate an approach to file management that's recognized internationally as being at the forefront of best practice. Dealing with international partners who comply with the Standard adds confidence to relationships between governments, businesses and with clients.

The information within ISO 15489 acknowledges that each organization will have very individual demands and requirements for its information, data or records. By providing a best practice framework to follow and apply to individual cases, this records management standard provides a good, although by no means exhaustive, process to follow.

The documents that comprise the ISO Standard 15489 are split into two sections.

- Part 1 takes a general overview of records and information management and examines the principles and methodology behind its adoption.

- Part 2 is more involved with the practicalities of moving towards records management compliance. It provides an in-depth, often step-by-step approach to implementing electronic records and information management.

5.2 Information Security Management

In considering the protective measures that should be put in place within e-Government systems, a risk analysis should be performed. This risk analysis must consider the intent, motivation and capability of sources of threat, the feasibility and potential frequency of methods of attack, the nature of vulnerabilities that may be exploited, the value of assets to be protected, the consequences of a successful attack, and the costs of any countermeasures.

Threat analysis examines the assets that require protection, the potential sources of threat and the likely methods of attack. The following are assets of e-Government based services which require protection:

a) The personal data relating to a client for any e-Government service must be protected against loss, damage, or unwarranted disclosure in line with the relevant data protection and privacy legislation.
b) The corporate information base of government in general and organizations offering e-Government services must be protected against loss, unwarranted disclosure or introduction of erroneous content.
c) The e-Government service (comprising the applications and delivery platforms) must be protected against threats to its availability and the integrity of the service offered.
d) Authentication credentials must be protected against forgery or unwarranted use.
e) Objects that represent monetary or other value must be protected against fraud. Some of the e-Government transactions are likely to result in cashable orders, which must be properly controlled, some may relate to the delivery of goods that can be misappropriated.

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other organizational and management processes.

1. ISO Standard 17799: Information Security Management

The ISO Standard 17799 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO 17799 contains best practices of control objectives and controls in the following areas of information security management:

- security policy;
- organization of information security;
- asset management;
- human resources security;

- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management;
- compliance.

The control objectives and controls in ISO 17799 are intended to be implemented to meet the requirements identified by the risk assessment. ISO 17799 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

The revised ISO 17799, "Information Technology: Security techniques - Code of practice for information security management", integrates the latest developments in the field to maintain it as the international standard code of practice. The modern interconnected e-government and e-commerce environments, with information now exposed to a growing number and a wider variety of threats and vulnerabilities, are the main beneficiaries of the standard.

This standard recognizes that the level of security that can be achieved purely through technical means is limited. The required level of security, established through assessing the levels of risk and associated costs through breaches of security, against the costs of implementing security, should always be driven by appropriate management controls and procedures. Information security management requires, as a minimum, participation by all employees in the organization.

ISO 17799 identifies the controls that form the starting point for information security. It covers the critical success factors, the organization of information security, asset management, human resources, physical and environmental security, communications and operations management, information systems acquisition, development and maintenance, incident management, business continuity management and compliance.

2. ISO Standard 18028: IT Network Security

There is a wide variety of safeguards from which IT security professionals can choose to secure their IT networks. The selection of the right safeguard determines network exposure (risks), the price/quality ratio of the network, and the flexibility to adjust to changing circumstances in a secure way. ISO 18028 provides a repository of threats, safeguards and mappings, providing organizations with guidance for network security.

ISO 18028-1 provides a ***process approach*** to network security management. It offers a risk-based framework, focusing on the selection of safeguards, the types of connections, their characteristics and trust as well as potential risks. It offers guidelines for the implementation and monitoring of network security.

ISO 18028-2 proposes ***reference architecture***. It is based on three components: security dimensions (services like access, control and authentication, but also privacy), security layers (infrastructure security layer, the services security layer and the applications security layers, like ftp, mail and http) and finally, security planes (management security plane, control security plane (signaling) and the end-user security plane).

ISO 18028-3 describes ***techniques for security gateways***, like packet filtering, security gateway components, like switches and routers, as well as security gateway architectures (like single and multi-staging gateways). It also provides guidelines for
selection and configuration of gateways and gateway components.

ISO 18028-4 describes types of and techniques for ***remote access connections*** (communication servers, LAN resources, etc). It contains guidelines for selection and configuration. It contains an overview of VPNs and VPN security objectives and requirements. It lists guidelines for the selection and the implementation of secure VPNs (including monitoring).

3. ISO Standard 18044: Information Security Incident Management

ISO 18044 provides advice and guidance on information security incident management for information security managers and for information system managers. This standard provides:

- information on the benefits to be obtained from and the key issues associated with a good information security incident management approach (to convince senior management and those personnel who will report to and receive feedback that the scheme should be introduced and used);
- information on examples of information security incidents, and an insight into their possible causes;
- advice and guidance with respect to the detection, reporting and assessment of information security incidents
- guidelines on responding to information security incidents, including the activation of appropriate controls for the prevention and reduction of, and recovery from, impacts,
- a description of the planning and documentation required to introduce a good structured information security incident management approach

Information Security Incident Management Process

Quick, co-ordinated and effective responses to an information security incident require extensive technical and procedural preparations. Information security incident responses may consist of immediate, short- and long-term actions. Any actions undertaken as the response to an incident should be based on previously developed, documented and accepted security incident response procedures and processes, including those for post-response analysis. The proposed approach for implementing adequate security incident management is based on the PDCA process model, the Plan-Do-Check-Act cycle that is at the heart of the ISO approach.

5.3 Software Development Process

ISO 12207 is an ISO standard for software life cycle processes. It aims to be 'the' standard that defines all the tasks required for developing and maintaining software.

Standard ISO 12207 establishes a process of life cycle for software, including processes and activities applied during the acquisition and configuration of the services of the system. Each Process has a set of outcomes associated with it. There are 23 Processes, 95 Activities, 325 Tasks and 224 Outcomes.

The standard has the main objective of supplying a common structure so that the buyers, suppliers, developers, maintainers, operators, managers and technicians involved with the software development use a common language. This common language is established in the form of well defined processes. The structure of the standard was intended to be conceived in a flexible, modular way so as to be adaptable to the necessities of whoever uses it. The standard is based on two basic principles: modularity and responsibility. Modularity means processes with minimum coupling and maximum cohesion. Responsibility means to establish a responsibility for each process, facilitating the application of the standard in projects where many people can be legally involved.

The set of processes, activities and tasks can be adapted according to the software project. These processes are classified in three types: basic, for support and organizational. The support and organizational processes must exist independently of the organization and the project being executed. The basic processes are instantiated according to the situation.

ISO 12207 offers a framework for software life-cycle processes from concept through retirement. It is especially suitable for acquisitions because it recognizes the distinct roles of acquirer and supplier. In fact, the standard is intended for two-party use where an agreement or contract defines the development, maintenance, or operation of a software system. It is not applicable to the purchase of commercial-off-the-shelf (COTS) software products.

5.4 Acceptable Use

Standards for acceptable use define the appropriate use of technology in the public sector, this includes the hardware, software, and communications equipment the Government of Belize provides. To prevent tarnishing the public image of Government of Belize when email goes out from Government of Belize the general public will tend to view that message as an official statement from the Government of Belize.

These standards also define the appropriate the use of any email sent from a Government of Belize email address and applies to all employees and agents operating on behalf of Government of Belize.

Standards for Acceptable Use

- ***Copyrighted Material:***
  - Users will not violate copyright laws and their fair use provisions through inappropriate use, reproduction and/or distribution of music, movies, computer software, copyrighted text and images on any GOB computer or computer network.
- ***Hacking Attempts:***
  - Users shall not use computers or network facilities to gain or attempt to unauthorized access to any computer systems.
  - Using programs intended to gain or attempt to gain access to unauthorized systems for any reason or purpose is strictly prohibited.
- ***Connections to the Network:***
  - Users shall not connect unauthorized equipment to Government of Belize equipment including, but not limited to, computers, laptops, handheld devices, docking stations, hubs, routers, printers or other equipment connected to any GOB network directly or via remote attachment or connections.
- ***Data:***

  Data Protection Principles/Guidelines: The standards for data protection are based on the following principles:

  1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under any relevant legislation.
7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside Belize unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

<u>Standards for Use of Data:</u>

- Users shall not prevent any other user who is the rightful owner from accessing data.
- All electronic data is the property of the GOB and the user is required to protect this information to the extent reasonably possible for the security and privacy of those involved. The user may disclose the data, provided that the user acts in good faith, in fulfillment of any obligations under any law and in compliance with a written directive from a duly authorized person.
- Users will not view or copy or attempt to view or copy data which has not been made available to them in the normal course of their duties.
- Should the user leave the employ of the GOB, travel outside their authorized work area or become incapacitated for a period of time, all GOB information is to be removed from portable devices immediately.
- Person from whom data is collected shall be informed of the provisions related to the collection, storage and disclosure of such data.

- ***Network Security:***
  - Users shall not disclose a password without authorization.
  - Users shall not make unauthorized attempts to circumvent data protection mechanisms or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
  - Computers connected to any GOB network should have adequate protection, such as the installation of Anti Virus Software.
  - No direct connection should be made from any GOB Network to any other Network (particularly the Internet) without an appropriately configured firewall at the point of connection. Of particular concern here are ADSL connections, which are 'always on' connections, but dial up connections must also be protected.
  - The Administrator for the respective GOB Network should be informed of all ADSL and other connections to external Networks, including the name and contact information for the Officer responsible for maintaining the associated firewall. This information is necessary for the coordination of an effective response when virus and other security alerts are received and will be shared amongst the various responsible Officers.
  - All workstations should have password protected screen savers activated or should be logged off when not in use. Workstations and other client machines should be shut down when not in use for prolonged periods.
- ***Software:***
  - Users will not violate terms of applicable software licensing agreements and intellectual property right laws.
  - Users will not knowingly or carelessly run or install on any GOB computer system or network, or give to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to computer viruses, Trojan Horses and worms.

- **Hardware:**
    - Disposal of Hardware: Users shall not displace/remove, modify, damage or destroy computer equipment without the relevant authorization as prescribed by the Audit and Finance Act. A department may dispose of computer related equipment that is no longer useful for any of the following reasons: cannot provide basic level of service; unused; cannot be upgraded to handle required software/hardware; damaged or broken; beyond economic repair or replaced with new equipment. Computer related equipment meeting any of the above criteria would be considered surplus.
    - Departments having surplus equipment shall not transfer to another department, sell, recycle, or dispose of equipment without first following the applicable provisions of the Audit and Finance Act.
- **Email:**
    - Any Government of Belize email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about ethnicity, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any GOB employee shall report the matter to their supervisor immediately.
    - Non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Government of Belize email account is prohibited. Virus or other malware warnings and mass mailings from Government of Belize shall be approved by the Chief Executive Officer of the Ministry before sending. These restrictions also apply to the forwarding of mail received by a Government of Belize employee.
    - Government of Belize employees shall have no expectation of privacy in anything they store, send or receive on any GOB email system. Government of Belize may monitor messages without prior notice. Government of Belize is not obligated to monitor email messages.
    - Users shall not forge the identity of a user or machine in any electronic communication.

- Users shall not transmit or reproduce materials that are slanderous or defamatory in nature, or that otherwise violate existing laws, regulations, policies or that are considered to be generally inappropriate in a workplace.
- Users shall not use another person's password or email address without authorization.
- Users shall not attempt to monitor or tamper with another user's electronic communication or read, copy, change, or delete another user's files or software without the explicit agreement of that user.

Any employee found to have violated any of the above provisions on standards for acceptable use shall be subject to disciplinary action, up to and including termination of employment.

6. Financing Mechanism

Like any government infrastructure project, e-government can be done in phases and the costs of implementation will depend on current infrastructure availability, supplier and user capabilities, and mode of service delivery (whether through the Internet or through telephone hotlines and one-stop shops). The more complicated and sophisticated the services the government wants to offer, the more expensive e-government will be.

The Government of Belize should focus initially on small, self-financing or donor financed projects, because e-government projects should be financially sustainable. Smaller projects with a clear effectiveness strategy and minimal initial investment are the most likely to be sustainable over the long term. For instance, Web sites and Web based systems are one of the easiest and cheapest ways to achieve high impact e-government with a minimum of investment.

Many E-government projects, however, are more often than not, long-term endeavors, requiring large capital infusion in software, hardware, infrastructure and training. A viable financing plan should not only pay for the immediate needs to jumpstart e-government; it should also consider its long-term financing options for the sustainability of the project.

Financing and technical assistance arrangements can be pursued with the Regional and International Agencies and Partners. In particular, cooperation with the private sector is to be encouraged in order to facilitate effective e-government. The key to e-government is to improve citizen access to service delivery, not further expand the role of government. GOB should not attempt to create products and services where public-private partnerships or private service providers can adequately provide these products and services more efficiently and effectively.

7. Legislative and Regulatory Framework

The successful implementation of e-government policies and processes can be significantly enabled by a proper legal framework for their operation. A requirement for e-government processes to be introduced and adopted is their formal legal equivalence and standing with the paper process. Many governments are now aware of the need for framework to provide for enforceable electronic transactions, both in the e-government sphere and for e-commerce, and have taken action. For example, the legal recognition of digital signatures is necessary if they are to be used in e-government for the submission of electronic forms containing sensitive personal or financial information (Basu, 2004).

Ideally, a legal framework that allows for the implementation of e-government processes and services will:

- Preserve basic public policy goals, such as privacy and security, retention, and public access to information.
- Provide the statutory basis of, authority for, and regulations related to the government processes and services that may be supplied electronically.
- Assign responsibility for and ownership rights to the data provided and accumulated electronically.
- Address the sharing of data collected by one government agency with other government agencies that require the same information.
- Clearly, define jurisdictional responsibilities related to intergovernmental transactions and business to government transactions.
- Provide a mechanism by which legal requirements are recognized and enforced.
- Provide a basis for the establishment of fees related to electronic processes and services.
- Identify the records that should be maintained, the period of retention and the required storage media.
- Not be technology-specific or favour one form of service delivery (traditional or electronic).
- Minimize costs and the potential for litigation[6].

[6] Basu, S. (2004). ***"E-Government and Developing Countries: An Overview"***. International Review of Law Computers & Technology, Volume 18, No. 1, Pages 109–132.

While the Government of Belize has enacted several key legislation: Electronic Transactions Act (2003), Electronic Evidence Act (2003), Freedom of Information Act (1994, amended in 2000), and the Archives and Records Service Act (2004), there are other critical areas which must be addressed if the E-Government Policy is to have any meaningful impact, in particular:

- Computer and Computer Related Crime/Computer Misuse: makes attempted or actual penetration or subversion of computer systems a criminal act and prohibits the unauthorized access, use of or interference to any program or data held in a computer and to a computer itself.
- Privacy and Data Protection: sets requirements for the proper handling and protection of personal information held within information processing systems and to protect the privacy of individuals in relation to personal data, to regulate the collection, processing, keeping, use and disclosure of certain information relating to individuals and to provide for matters incidental thereto or connected therewith.

8. Institutional Framework

8.1 IT/IM Professional Stream in the Public Service

This policy proposes a reclassification which would seek to establish a rational and logical career path for Information Technology and Information Management professionals in the Belize Public Service, catering for various streams, in order to support the present and future IT/IM requirements of the Government of Belize. Firstly, it should be noted that many anomalies and inconsistencies presently exist with respect to the classification of Information Technology and Information Management positions in the Public Service. This has arisen due to well-intentioned, but disjointed and ad-hoc creation of IT related positions to meet the needs of Agencies from time to time.

The primary objectives of the revised classification of IT posts are to:

- attract and retain competent and highly skilled Information Technology Professionals in Public Service;
- ensure appropriate levels of job satisfaction and motivation, through the provision of clearly defined career paths for upward mobility; and
- promote consistency with other professional streams in the Public Service.

8.2 ICT and E-Government Functions

It is recommended that the Office of Governance, as the Government of Belize organization with the mandate for ICT/E-Government, strengthen its' capacity to function as the national ICT Executing Agency. This function should be undertaken in close collaboration with the ICT sections/departments/units of other Government Ministries/Agencies as well as with other ICT-related organizations in the public and private sector. Every effort should be made to avoid the unnecessary duplication of functions by optimizing the utilization of ICT resources and leveraging ongoing initiatives and capabilities in the wider public sector.

The Office of Governance will be responsible for coordinating National ICT initiatives and projects and facilitating the implementation of ICT related programmes. The Agency will also

have the responsibility for developing National ICT Standards and Guidelines and will undertake public awareness and education role in the area of ICT and information management.

The specific functions to be undertaken can be classified as: 1. General ICT/ICT related and 2. Technical functions:

8.2.1 General ICT/e-government Related Functions:

1. Strategy: developing strategies and planning for ICT within Government and providing a framework for programme management for implementation, to support the Government's objectives for improved public service delivery and administrative efficiency, in the context of Public Sector Modernization and good governance.

2. Process Analysis and Process Reengineering: for key Public Sector operations that are or can be ICT-enabled and have the potential to add value & directly impact on the level of citizen & business satisfaction with public sector services.

3. ICT Finance: in partnership with Ministry of Finance, monitoring major ICT projects in Government and advising on major investment decisions.

4. ICT Human Resources: promoting and advancing the ICT Profession in Government and leading its professional development.

5. Special Projects: undertaking continuous assessment through policy and strategy studies in the advancement of the E-Government and improved governance agenda.

6. Research: identifying and communicating key technology trends, opportunities, threats and risks for Government and for the furtherance of ICT for economic and social development.

8.2.2. Technical Functions

1. Feasibility Studies: conducting operational, technical and financial feasibility of proposed ICT programme and projects, including Systems Analysis and Design;

2. System Architecture: providing policy, design, standards, governance, advice and guidance for ICT in Government; commissioning Government-wide infrastructure and services; the implementation of the new National ID Card and addressing issues of systems integration across the Public Service and Quasi-governmental agencies and statutory bodies;

3. Network Infrastructure: Upgrade and rationalize the use of Local Area and Wide Area Networks, including: the implementation of a voice over IP network; coordination and optimization of the island-wide frame relay networks; implement and monitor standards for the secure transmission and storage of data; and the configuration of wide area and local area networks (WANs & LANs): segmentation/partitioning issues, network administration & support; rationalize the assignment of IP addresses;

4. Web Services: manage the Government of Belize Portal, develop and manage an Intranet/Extranet and web based email; Domain Name Management: country-code top-level domain names (.bz) & function indicator (.gov)[7]; manage policies on Web hosting and integration of public sector web sites, including quasi-governmental agencies and the facilitation of government online services: G2G,G2E, G2B & G2C.

5. Security: oversee Government ICT security policy, standards, monitoring and assurance, and contingency planning for critical national infrastructure;

6. Databases/Software Applications: undertaking Systems auditing of key databases and systems; Design & assist in building and upgrading databases/systems to support the data

[7] Management of country-code top-level domain names (cc-TLDs): Country-level domain names establish the online identity of a country and its people. Given the importance of the Internet to the political, social and economic development of countries, it is essential that the management of the cc-TLD "serve the best interests and desires of the local Internet community, including governments".

and information requirements of Agencies; promote the use of open source software and the implementation of standards & policies for: Data storage and information sharing; Data Integrity; Disaster Recovery; and Data Warehousing & Archiving.

7. Data, Information and Knowledge Management: Develop and implement Policies and procedures on records management: data, information & knowledge.

8. Innovation: providing high-level advice to Government bodies on innovative opportunities arising from ICT to improve efficiency and to enhance competitiveness in the global information society and knowledge economy.

8.3 ICT and E-Government: Staffing

The staffing of the Office of Governance should be significantly enhanced to enable the coordinated, systematic and purposeful approach, towards the attainment of strategic and policy objectives, as well as the execution of the more technical functions outlined above.

9. Human Resource Development and Capacity Building

Connectivity itself is necessary but not sufficient, to ensure access. Access requires that there be ***human resource capacity*** to access, use and even produce the technologies; that the technology is accessible in terms of language and capabilities; that locally relevant content is available and that there is a focus on raising awareness[8]. Of critical importance is developing the levels of understanding and capabilities with respect to ICTs.

9.1 Public Sector

In order to advance the e-Government agenda, capacity building in the Pubic Sector will be undertaken at three (3) levels:

- Ministerial and senior management;
- Information Technology & other technical personnel; and
- End-Users

It is recommended that detailed Training Plans be developed based on the findings of a 'Training Needs Analysis', to be conducted by the Office of Governance for the three categories listed above. However, capacity building in the above areas should be guided by the following principles:

9.1.1 Ministerial and Senior Management

A wealth of literature espouses the need for top management support as a key criterion for information technology implementation success in the public sector[9]. A fundamental reason for the contention that enhancing top management understanding and knowledge is imperative for advancing the e-government agenda is the very nature of public sector bureaucracies generally, and in developing countries in particular. Some of the significant characteristics identified in developing country public sector organisations are the high level of risk aversion; disinclination towards dramatic or rapid changes; rigid,

[8] United Nations ICT Taskforce Series 3 (2003), The Role of Information and Communications Technologies in Global Development: Analyses and Policy Recommendations. Edited by A.B. Haqqani.

[9] Bajjaly, 1999; Montealegre, 1999; Davidson, 1997; De Conti, 1998; Coulson-Thomas, 1998; McKeen, Guimaraes and Wetherbe, 1994).

authoritarian, bureaucratic structures; and a lack of incentives for innovation and changing the status quo.

Successful and meaningful e-Government initiatives in the Belize Public Sector will require substantial IT-enabled organisational process changes. The required level of resources and emphasis assigned to IT related initiatives; the extent to which these activities are integrated into the operations of the organization; and the speed and resolve (sense of urgency) with which this is executed invariably depends on the direct influence and actions of top management. This influence and actions will only be forthcoming, with a greater level of management understanding and knowledge of the potential of the new information and communications technologies. It should also be emphasized that such knowledge does not need to be centered on the more technical aspects, but should deal with the management and organizational issues relating to the adoption and implementation of ICTs, as well as enhancing managerial capabilities for the use of relevant ICT applications for greater personal productivity and efficiency.

9.1.2 Information Technology and Technical Personnel

- Notwithstanding the Training Needs Analysis to be conducted, it is recommended that in the short term, training and capacity-building activities should be pursued in the following areas:

i. Change management and Business Process Reengineering
ii. Reporting tools
iii. Network Infrastructure: Wide Area Networks running on Frame Relay, Fibre Optic and Wireless platforms
iv. Web Developer/ Designer/ Programmer, Web Server Management and Domain Name Management Capacity Building
v. Specific training where necessary, such as: CompTIA A+ , Linux+, Network+ Certification, CISCO Certified Network, Certified Internet Webmaster (CIW) - Master CIW Designer Training.

The above training should be arranged on an in-service/in-house basis, i.e. bringing in a Trainer in order to maximize the number of persons who can benefit from the training opportunity. This training should always include a 'Training of Trainers' component, so as to ensure sustainability and maximize knowledge transfer. Training opportunities arranged overseas: with other countries, international agencies and other Partners, should be done on the understanding that participants will conduct training sessions (workshop format or structured on-the-job knowledge/skills transfer sessions) upon their return.

9.1.3 End Users

Empirical Studies of the relationships among: Information Systems acceptance by end-users, end-user training, and effectiveness in the performance of IT-enabled tasks indicate both the importance of training and end-user information system (IS) acceptance and strong positive relationships between end-user skill levels and job performance.

It is therefore recommended that the Training Plan for end-users, based on the results of the Training Needs Analysis, be implemented as a matter of urgency. Notwithstanding the Training Needs Analysis to be conducted, it is recommended that in the short term, training and capacity-building activities should be pursued in the following areas:

- Microsoft Office Specialist Training

  Microsoft Office Specialist programme is the premier Microsoft desktop productivity certification. It is a globally recognized standard that validates computer desktop skills and is useful for validating expertise with the Microsoft Office suite of business productivity programs. This program is highly recommended for the Belize Public Service due to the fact that, notwithstanding the widespread use of Microsoft Office applications in the Public Service, the functionality and features of the software suite is underutilized, with a consequent negative impact on employee productivity, efficiency and effectiveness.

- The International Computer Driving Licence (ICDL)

  The International Computer Driving Licence (ICDL) is a global competency standard endorsed for computer literacy in over one hundred and forty (140) countries. The ICDL is designed for a person to 'drive' a computer with the same ease as they might drive a car. Its aims are to: raise the general level of competency in IT; improve productivity at work; reduce user support costs; enable employers to invest more efficiently in IT, and ensure that best practice and quality issues are understood and implemented.

  The ICDL is not a "training course" per se, but rather a competency standard that is acknowledged through testing. It is based on the successful European Computer Driving Licence scheme (ECDL).

9.2 Private Sector

This Policy promotes, as an essential component as the capacity building effort, the use of ICT for wider economic development. Indeed, the successful delivery of an essential component of the e-govenrment agenda, i.e. government to business (G2B) is contingent on the awareness, capacity and willingness of the private sector to adopt and utilize ICTs. The main policy measure in this regard will be to:

- engage private sector organisations to assist in programmes to support small businesses with a view to enable them to better invest and use ICTs.
- encourage the development and establishment of accreditation and quality assurance processes for ICT training at a national level.

9.3 Citizens

The primary challenge to the further development of e-government initiatives and more generally, the advancement of the information society in the Belize, is the need to ensure that ICTs are accessible to all sectors of the society and is used to bridge existing socio-economic gaps. Given the relatively low level of online penetration in Belize, as in many Caribbean countries, compounded by the wide disparities in internet access within these societies, strategies for enhancing e-citizenship must have a strong 'off-line' component, focused on awareness and

capacity building. Similar to the use of advertising in traditional media by online, pure-play internet companies like Amazon.com, e-citizenship and participation in the information society in Belize must be fostered by the use of traditional sources - radio, television and print media, as well as creative off-line strategies to engender interest and build capacity.

It should be noted that the impact of ICT on socio-economic development has been the source of debate and interest in many countries around the world. The advancement of the 'ICT for Development' agenda, e-citizenship or e-participation, to a large extent, is dependant upon the ability and willingness of persons to use the technology in various aspects of their lives. It is essential, therefore, that the level of penetration of computers and the internet among the general population be assessed and used as the basis for ICT and e-government policy formulation.

This would increase the likelihood that ICT would have a meaningful impact on socio-economic development and specifically address any existing disparities in access to information, services and ultimately to opportunities for income generation and wealth creation within respective communities and societies across the region. Studies and analysis undertaken by Trinidad and Tobago and Saint Lucia are good examples of this approach.

The policy position of the government of Belize will promote two specific approaches:

(1) Hosting of an Internet Awareness Programme

The main objectives of such a programme would be: to increase awareness of the possibilities of the Internet among the young and the old, and among private and public sector workers in a fun environment; to initiate and expand an electronic network between people within and across national borders and language barriers and to host an event with a Caribbean flavor, promoting education and training in the usage of the Internet as a valuable resource for economic development and social interaction in an enjoyable way.

Internet Fiesta is an activity to promote Internet Awareness. Started in Europe about five years ago, it has been included in the events calendar of many countries around the world. Under the theme: "Internet for All", Internet Fiesta 2004 was implemented in

four islands in the Eastern Caribbean: St. Lucia, Antigua & Barbuda, St. Kitts & Nevis and St. Vincent, in collaboration with the French territory of Martinique and the local private sector in each country, in particular the ICT and telecommunications sectors and training institutions/education providers.

(2) Implementation of a Community Technology Programme.

Following from the 'one-off' annual event - Internet Fiesta, there needs to be a sustained, ongoing effort at capacity building at the 'grass roots level. This can take the form of a comprehensive community technology programme (CTP). The CTP can create an enabling environment for community members of all ages, enabling them to participate and taking advantage of the opportunities that arise in this technological era.

The objectives of the programme would be to: make computer training and Internet access more readily available to the masses; strengthen parents' understanding of, and support for the use of computers in schools; increase and improve the technological literacy of community members; provide opportunities for social connections and communication; and facilitate the development and transformation of regular Community Centres into Community Resource Centres.

These Resource Centers, will serve as Community Access Points are community or public buildings where computers, printers and scanners are installed for persons in the community to use either free of charge or for relatively low costs. It is hoped that all the computers would have broadband connection to the Internet.

The CAPs are intended to help rural and disadvantaged communities finance and implement projects aimed at improving their daily lives through the use of ICT. It is hoped that these CAPs would be characterized as being demand-driven development programme where decisions are taken by the communities themselves and funds are allocated according to priorities decided on by the community. Furthermore these CAP seek to build capacity of communities by enhancing existing skills and facilitating the acquisition of new skills. To ensure the success of these initiatives, the rollout of CAPs should be done alongside an awareness campaign in target communities on the role of ICT as a tool for development and empowerment.

10. Policy Statements: E-Government Services

The three types of e-government services are Government-to-Citizen (G2C), Government-to-Government (G2G) and Government-to-Business (G2B).

10.1 Government to Citizen (G2C)

G2C includes information dissemination to the public, basic citizen services such as license renewals, ordering of birth/death/marriage certificates and filing of income taxes, as well as citizen assistance for such basic services as education, health care, hospital information, libraries, and the like.

- The GOB will enhance cost effectiveness and reach of government services by enhancing the provision of public services, and by focusing on inclusivity and the development of integrated solutions

- The process of selection and prioritization of G2C e-government services will be done on a demand-driven, citizen-centric basis.

- The GOB will seek to increase levels of access to the Internet and web-based services by providing opportunities for connectivity through cost-effective and convenient/citizen-centric methods.

- The GOB of Belize will publish and promote its' privacy and data protection policies so as to enhance levels of citizen/user trust and confidence in the delivery of e-government services.

- In this regard, the GOB will pursue the early adoption of the following ISO Standards:
    - Data and Information Management - Records Management (ISO 15489)
    - Information Security Management (ISO 17799)
    - IT Network Security (ISO 18028)
    - Information Security Incident Management (ISO 18044)

10.2 Government to Government (G2G)

G2G services take place at two levels: at the local or domestic level and at the international level. G2G services are transactions between the central/national and local governments, and between department-level and attached agencies and bureaus. At the same time, G2G services are transaction between governments, and can be used as an instrument of international relations and diplomacy.

The GOB will:

- Conduct process analysis and reengineering of key Public Sector operations: in particular those already employing Information and Communication Technology at the operational level and those processes that add value and directly impact on the level of citizen and business satisfaction with public sector services.

- Establish a Web Portal with consistent design and layout (with (similar look & feel) for each government agency and /or links to other sites in the Public Sector.

- Develop and execute comprehensive public sensitization campaign with respect to the GOB Web Portal.

- Establish a comprehensive management information system (MIS) for sharing information of all government agencies to the public.

- Integrate and upgrade Online Services and Web services in the Public Sector, including:
  - Domain Name Management: Establishment of Registry to manage the country-code, top-level indicator (.bz) and function indicator (.gov);
  - implementation of policies and harmonized practices on Hosting and management of government web sites;
  - implementation of a Intranet for the entire Public Service and an Extranet for access by quasi-governmental and relevant external agencies;

- coordination and provision of support for the delivery of government services online: Government to Business (G2B); Government to Citizen (G2C); Government to Government (G2G); Government to Employee (G2E);
- link back-end systems to government websites to enable the creation of dynamic, interactive online services, with access to real time data and processing capabilities.

- Develop and integrate the GOB Wide Area Network (WAN).

- Conduct a sustained HR training programme to build proficiency in the use of ICT as well as high-end ICT knowledge and skills in the Public Service

- Review and upgrade of databases/systems and back-end processes, in the Public Sector, including:
  - extensive systems auditing of key databases and systems;
  - design and assist in the building of databases and other back-end systems to support the data and information requirements of Agencies;
  - implementation of standards & policies for: data storage and information sharing; Data Integrity; Disaster Recovery; and Data Warehousing & Archiving.

10.3 Government to Business (G2B)

G2B transactions include various services exchanged between government and the business community, including dissemination of policies, memos, rules and regulations. Business services offered include obtaining current business information, downloading application forms, renewing licenses, registering businesses, obtaining permits, and payment of taxes. The services offered through G2B transactions also assist in business development, specifically the development of small and medium enterprises. Simplifying application procedures that would facilitate the approval process for SME requests would encourage business development.

On a higher level, G2B services include e-procurement, an online government supplier exchange for the purchase of goods and services by government. Typically, e-procurement Web sites allow qualified and registered users to look for buyers or sellers of goods and services.

The GOB will:

- encourage the adoption and use of ICT in the private sector to increase efficiency, competitiveness and market access, particularly small, medium, micro scale businesses in rural and urban areas.

- The process of selection and prioritization of G2B e-government services will be done on a demand-driven, user-centric basis.

- The GOB will encourage the adoption of the following ISO Standards by private sector organizations, in particular those which have the potential to engage in G2B e-government interactions and e-commerce/e-business activities:
    - Data and Information Management - Records Management (ISO 15489);
    - Information Security Management (ISO 17799); IT Network Security (ISO 18028); and Information Security Incident Management (ISO 18044).

- The GOB will seek to increase levels of access to the Internet and web-based services by providing opportunities for connectivity through cost-effective and convenient/user-centric methods so as to increase market information and reduce transaction costs for busines