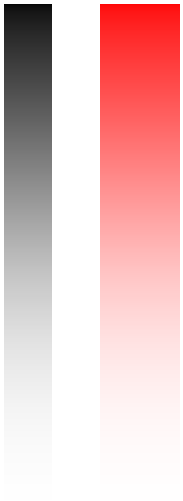
REPUBLIC OF TRINIDAD AND TOBAGO



Policy and Procedural Guidelines for

The e-Government Portal and Web-based, Enterprise-wide Applications

MINISTRY OF PUBLIC ADMINISTRATION AND INFORMATION

Version 1.0
April 21, 2006

1.1 Policy Name

This policy may be referred to as the **e-Government Portal and Web-based, Enterprise-wide Applications Policy**

1.2 Target Audience

This policy is intended for the public service agency employees and consultants using the services offered by the e-Government Portal and using the government corporate applications both "locally" within a particular public service agency via their Local Area Network (LAN) and/or "distributed" via the government Wide Area Network (WAN) infrastructure. The policy assumes that the relevant networking/support infrastructure is in place.

1.3 Policy Purpose

Information is a critical asset for the operational business functions and service delivery of the Government of the Republic of Trinidad and Tobago (GoRTT). Any person working for GoRTT in a part/full-time capacity or under a contractual agreement conducting business for, with, or on behalf of GoRTT ("Employees and Consultants"), as a condition of employment and engagement, is responsible for ensuring the security of this asset.

The wide array of resources with regard to information and online web-based services available by way of the e-Government Portal and all web-based enterprise-wide applications, expose GoRTT to a variety of content implications. These implications include:

a) The availability of the appropriate content;
b) The validity or accuracy of this content for strategic decision making; and
c) For the purpose of academic research, the currency of the content for use in the preparation of various papers and articles that drive the entire decision making process within government.

It is in response to these implications, and others, that this policy was developed.

1.4 Policy Overview

The e-Government Portal and all Web-based Enterprise-wide Applications are essential business tools for GoRTT. The objective of this policy is to minimize the risk to GoRTT arising from use of the Portal and the web-based enterprise-wide applications without unduly hindering GoRTT's ability to deliver quality services internally and to the public.

GoRTT must control and justify the use of the e-Government Portal and all web-based enterprise-wide applications. This policy will address the following objectives:

a) to standardize online web-based services to employees and consultants in order to provide the means and tools necessary to fulfill their tasks and perform their job function activities in an effective and efficient manner;

b) to ensure accountability for the actions performed by each user, consistency with GoRTT's expectations, and compliance with published policies; and
c) to protect GoRTT's information system resources from abuse.

1.5 Policy Maintenance History

Revisions of this policy are to be tracked and detailed below:

Date	Change details	Author	Version
20-Nov-03	Initial Draft	MPAI	0.0.1
27-Jan-05	Policy Revision inclusive of comments and recommendations	MPAI	0.1.0
23-Sept-05	Minor corrections to prepare document for presentation to Cabinet for approval	MPAI	0.2.0
05-Oct-05	Updated to include comments from PS	MPAI	0.3.0
31-Oct-05	Updated to include review comments from DPS	MPAI	1.0.0

1.6 Administration (Policy Ownership, General Responsibilities)

1.6.1 ***Policy Ownership***

This policy document is prepared and maintained by the Ministry responsible for overseeing and managing GoRTT's Information and Communications Technology (ICT) function. It is the responsibility of the individual public service agencies to assume responsibility for the implementation and enforcement of this policy to ensure compliance.

The policy will be reviewed to ensure that it is addressing current issues with respect to publications and use of content on the Portal, use of applications and the requirements of GoRTT. All revisions or modifications to this policy are the responsibility of the Ministry referred to above. Questions concerning the policy and suggested revisions should therefore be directed to this Ministry.

1.6.2 ***General Responsibilities***

Ministry responsible for overseeing and managing GoRTT's ICT function

Responsible for endorsing and supporting the e-Government Portal and all web-based, enterprise-wide applications policy; for ensuring that the Portal and web-based, enterprise-wide applications retain a high profile within GoRTT, at the public service agency level; and for guaranteeing that appropriate budget and personnel resources are available for the ongoing development, implementation and review of the policy. This Ministry must approve major initiatives aimed at enhancing the e-Government Portal and all web-based, enterprise-wide applications.

Employees and Consultants

All GoRTT employees and consultants are expected to respect this policy in spirit and comply with the statements contained herein.

Managers and Supervisors

Responsible for ensuring that the employees and consultants under their direction comply with this policy, specifically to:

- Ensure that employees and consultants understand the Portal and all web-based, enterprise-wide applications policies, procedures and responsibilities;
- Approve appropriate computer, information and application resource access;
- Review, evaluate and respond to all Portal and web-based, enterprise-wide application violations reported by employees and consultants and take appropriate action;
- Ensure all Portal and all web-based, enterprise-wide application procedures are in place to protect the content and information systems assets under their control. Such procedures would include physical access control, virus protection for workstations, all (information systems) web-based applications, local area networks, etc.; and
- Continuously keep Content Managers, or persons with responsibility for this function, informed on changes to access rights to publish content and to use web-based, enterprise-wide applications (information systems), including the removal or creation of specific content for publishing to the Portal.

Corporate Communications Units

- It is assumed that all public service agencies have a *"Corporate Communications or Public Relations Unit"*, if not, one should be established for the responsibility of management of web-based content within that agency.
- The position of *"Content Manager"* should be established within the agency's organizational structure either under the *"Corporate Communications or Public Relations Unit"* with responsibilities for the agency's content management issues and publishing to the e-Government Portal and/or any web presence on the Internet/Intranet.
- The Content Manager must liaise with the IT Department of his/her agency on web-based content issues for publishing to the e-Government Portal.
- The agency responsible for GoRTT's ICT function will be the overall coordinator of content for the e-Government Portal.

Information Owners

GoRTT computer systems and information re government specific content, which need certain protection, must have a designated 'Information Owner'. Information owners are responsible for their information and, in particular, for its accuracy and classification according to any future GoRTT policy on Data Classification and Control.

Public Service Agency IT Management and Technical Staff

- Responsible for implementation of the e-Government Portal and web-based, enterprise-wide application policies within their agency, ensuring that employees and consultants who have access to and use of GoRTT's computers, content, information systems and network systems comply with this policy and report violations to the Ministry with responsibility for GoRTT's ICT function or any agency it may designate to monitor this function.
- Each IT Division or Unit within the public service agencies is responsible for handling all violations re the e-Government Portal, and must report all violations to the agency responsible for ICT in the public service.
- A designated officer within the IT Division or Unit must liaise with the Content Manager or the officer with the responsibility for content management from the Corporate Communications Unit with reference to web-based content issues.

1.7 Compliance

All persons within GoRTT, and acting on behalf of GoRTT, are responsible for the security of GoRTT information assets entrusted to them.

- GoRTT employees and consultants are not to disclose confidential or sensitive information to third parties.
- Users of the system will restrict their access and use of the system to the intended purpose.
- GoRTT will ensure that use of company computing and network resources does not infringe criminal or civil laws, such as laws regarding the storage or transmission of libelous, indecent or offensive material.
- Employees and consultants must be aware that there are consequences for intentional misuse of GoRTT resources. Violations of this policy may lead to disciplinary action in accordance with governing Human Resource policies.

1.8 Policy Issues and Considerations

1.8.1 e-Government Portal / Agency Web Sites re Content

Developing web content policies and requirements for the e-Government Portal and agency websites is an ongoing process, requiring structure. The Ministry with responsibility for GoRTT's ICT function should have the Corporate Communications Units/Public Relations Units of all agencies meet at regular intervals:

- To create processes;
- To approve common content and links;

- To coordinate cross-agency portals; and
- To require agencies to report progress and compliance with web content policies and requirements.

1.8.2 Web-based, Enterprise-wide Applications Usage: (Local and Distributed)

- The use of web-based, enterprise-wide applications is a requirement for all managerial and operational staff to perform their daily tasks with efficiency and effectiveness, on a continuous basis.
- The Ministry with responsibility for GoRTT's ICT function must ensure that the appropriate standards, procedures and guidelines, once developed, are understood across all public service agencies so that all stakeholders benefit from the capabilities of these applications.
- The owners of the agency-specific, enterprise-wide applications will be responsible for ensuring that application-specific training is provided.

1.9 Procedural Guidelines

1.9.1 e-Government Portals

1. **Citizens must be able to identify official e-Government portals/websites and trust that those websites will provide current and accurate government information**.

   - The e-Government portals/websites must use government domains, follow basic common linking practices and be current.

2. **The e-Government portals/websites must be authored and organized from the public's perspective.**

   - Content must be organized in ways that make sense to citizens and other intended audiences.
   - Homepages must be authored and organized from the viewpoint of users.
   - Government websites should not be used for employee information.
   - The e-Government portals/websites must use basic common content, terminology and placement.
   - Agencies must measure customer satisfaction and usability of government websites.

3. **The e-Government portals/websites must be designed and authored to ensure they are usable and easily accessible**

   - The e-Government portals/websites must be user-friendly and customer oriented i.e. providing easy access, be authored in plain language, have consistent navigation, have a search engine, and use standard metadata.
   - Public websites must provide access to documents in standard file formats and provide appropriate access to data.

- Agencies must inform audiences of website changes and ensure continuity of operations during emergencies.

4. **In order to promote a seamless Government, public service agencies must work to simplify and rationalize information across the government.**
   - Government websites should avoid duplication and link to the appropriate government-wide portal(s).
   - Agencies must collaborate in developing government-wide portals.
   - Government websites must link to the e-Government Portal and link back to the website's homepage from every subordinate page.

5. **The responsibility for updating the e-Government Portal content sits with the Minister responsible for the government ministry that is providing the content.**
   - Such information (content) will require the approval of the Minister or the Head of independent agencies that are providing content for the e-Government Portal.

6. **Content on the e-Government Portal will be updated on a daily basis or as information is provided by the individual departments.**
   - All officers designated to update the content of the e-Government Portal must be trained to use the official Content Management System installed to perform this task.

7. **Government agencies/organizations must continue to comply with existing laws, regulations and policies that relate to ICT.**
   - Existing requirements include: privacy; security protocols; accessibility; Freedom of Information; information quality; copyright, trademark, and patents; The Computer Misuse Act; Integrity in Public Life Act; The Data Protection Bill (not yet submitted to Parliament) and the Electronic Transaction Bill (not yet submitted to Parliament).

1.9.2 Web-Based Enterprise-wide Applications

The "*Critical Issues*" that will apply to web-based, enterprise-wide applications are:

1. **Responsibility**

   The Ministry with the responsibility for GoRTT's ICT function must be consulted on all government, web-based, enterprise-wide applications that are accessible via the e-Government Portal. This will include the purchasing, installation and upgrading of the software for use by all public officers across the public service.

2. Security and Control

In addition to the policy statements outlined in the "Policy and Procedural Guidelines for Network Security and Access Control", security for web-based, enterprise-wide applications will include user authentication and customization restrictions.

- Users are required to have a username and password that will authorize their use of the application.
- Users are not permitted to customize the applications in any way to suit their individual needs unless they are authorized to do so. All customizations must be performed by the relevant application owner, assigned the responsibility to do so.

3. Accessibility

- Government officers will all have access to at least one web-based, enterprise-wide application, namely E-mail. Users are required to adhere to the "Policy and Procedural Guidelines for E-Mail and Internet Usage"
- Limited access will be given to users who are required to perform their duties using certain applications, for example - the Financial Management Information System (FMIS), the Human Resources Information Management System (IhRIS), the Integrated Government Payroll System (IGP), and the Electronic Document Management System (EDMS).
- All web-based, enterprise-wide applications will be accessible via the e-Government Portal.

4. Installation and Control

- The installation of all web-based, enterprise-wide applications must be done in consultation with the agency responsible for GoRTT's ICT function.
- Users are not allowed to uninstall or remove any government application whether web-based or stand-alone from their PC's location or workstation.
- The officer(s) in charge of the installation and removal of government applications must use the proper procedures and standards to successfully perform these tasks.

5. Data Integrity

ICT Officers or Officers with the responsibility for information and/or the management of information from respective public service agencies must:

- Ensure that data integrity is maintained for the different datasets residing in their various databases with respect to the software applications specific to that ministry;

- Ensure that frequent backups are done in accordance with the prescribed standards for the public service, this being a key method for maintaining data integrity;
- Be aware of the various "*threats to data integrity*" and therefore seek to rectify any foreseeable problems that may occur; and
- Employ all relevant precautions and or derive systematic procedures to avoid threats to data integrity as outlined in any future GoRTT policies/standards for the public service.

6. Business Continuity

Any business organization including government business must have a clear "*Disaster Recovery Plan (DRP)*" in place. A major component of this plan must include the procedures and or methodologies for the recovery of lost or corrupted data at the time of disaster or after a disaster occurs.

This policy statement assumes a disaster recovery plan with the appropriate "*Information Disaster Recovery Section*" is included within the DRP that is developed by each public service agency.

- ICT Officers or Officers with the responsibility for information and/or the management of information must have full knowledge of the DRP that has been drafted and implemented for their agency.
- All agencies must adhere to the formal procedures outlined in their DRP with specific reference to Information Disaster Recovery should a disaster occur.

This will ensure that delays in government business services are kept at a minimum and quality business services are continued.

7. Support and Maintenance

The Ministry with the responsibility for GoRTT's ICT function will:

- Update and/or customize, where necessary, the web-based, enterprise-wide applications accessible via the e-Government Portal, as they become relevant to the growing demand by the employees and consultants;
- Maintain all enterprise-wide application software with specific reference to software version control including software patches; and
- Provide overall administrative and technical support re web-based, enterprise-wide applications for all agencies as the need arises.

2.0 Glossary or Terms

For ease of use and overall understanding of the technical terms of this policy, a glossary or terms is provided.

1	e-Government	The use of electronic devices and the application of information and communications (digital) technology to support and automate the operations/functions of government business processes, providing quality services to the citizenry.
2	Portal	A second generation web presence with a single point of entry or "*gateway*" for accessing an organization's online web-based services via the World Wide Web and the Internet.
3	e-Government Portal	A single point of entry or "gateway" for citizens, public officers, visitors and businesses to access government "*online*" services via the World Wide Web and the Internet.
4	Local Area Network (LAN)	A network that is located in a small geographic area, such as an office, a building, a complex of buildings, or a campus, and whose communication technology provides a high-bandwidth, low-cost medium to which many nodes (computers, servers, routers, switches printers, copiers etc.) can be connected.
5	Wide Area Network (WAN)	A network spanning a large geographical area. Its nodes can span city, state or national boundaries. It uses circuits provided by common carriers.
6	Infrastructure	The structured arrangement of physical components that define a communications network including cabling, routers, switches and computers.
7	Online	Being connected to the Internet via the World Wide Web.
8	Web-based	An Information system that is only operational or can only be used via the World Wide Web.

9	Web-enabled	The version of an information system that is for use via the World Wide Web
10	Enterprise-wide	A macro perspective of the integration of all branches of a business firm or government organization.
11	Application Software	Modular computer programmes designed and developed for a specific purpose with specific groups of end users in mind.
12	Enterprise-wide Application Software	A computer program that was designed and developed for access to all end-users of branches of a business firm or government organization.
13	Network	A series of points/nodes connected by communication circuits.
14	Network Security	The relevant controls that are imposed on possible threats re disruption, destruction and disaster to a networked environment, the management of these controls and the assessment of risks for the implementation and operationalisation of an appropriate network security plan.
15	Content Manager	An officer with the major responsibility of managing all aspects of, and the issues arising from, matters dealing with web-based content.
16	ICT (Information and Communications Technology)	The integration of telecommunications tools, devices and systems to communicate and manage information across the globe.
17	IT (Information Technology)	The computer tools and digital devices used in supporting the management of information together with the information systems that are designed and developed for the management of information.
18	Authentication	A security method of guaranteeing that a message is genuine and that it comes from the source indicated. It ensures and proves who you are.
19	Customization	To change or alter specific functions of a system

		or device to the needs of a user or group of users.