TRINIDAD AND TOBAGO GAZETTE
(EXTRAORDINARY)

VOL. 45 Port-of-Spain, Trinidad, Monday 4th September, 2006—Price $1.00 NO. 143

1600

SUPPLEMENT TO THIS ISSUE

THE DOCUMENTS detailed hereunder have been issued and are published as a Supplement to this issue of the *Trinidad and Tobago Gazette:*

Legal Supplement Part B—

Resolution—(Legal Notice No. 182 of 2006).

Proclamation—(Legal Notice No. 183 of 2006).

Notice of Submission for Public Comment on an Environmental Impact Assessment Report submitted by Ecoengineering Consultants Limited on behalf of the National Gas Company of Trinidad and Tobago Limited—(Legal Notice No. 184 of 2006).

1601

APPOINTMENT AS TEMPORARY MEMBERS OF THE SENATE

IT IS HEREBY NOTIFIED for general information that, under the provisions of section 40(2)*(c)* and section 44 of the Constitution of the Republic of Trinidad and Tobago, His Excellency the President, acting in accordance with the advice of the Prime Minister, has appointed PROFESSOR DAVID PICOU, to be temporarily a Member of the Senate, with effect from 4th September, 2006 and continuing during the absence from Trinidad and Tobago of Senator DR. EASTLYN MCKENZIE.

H. HEMNATH
Secretary to His Excellency the President

4th September, 2006.

1602

IT IS HEREBY NOTIFIED for general information that, under the provisions of section 40 and section 44 of the Constitution of the Republic of Trinidad and Tobago, His Excellency the President, acting in accordance with the advice of the Prime Minister, has appointed MRS. JOAN HACKSHAW-MARSLIN, to be temporarily a Member of the Senate, with effect from 5th September, 2006 and continuing during the absence from Trinidad and Tobago of Senator JOAN YUILLE-WILLIAMS.

H. HEMNATH
Secretary to His Excellency the President

1st September, 2006.

1603

APPOINTMENT AS A MEMBER OF THE INTEGRITY COMMISSION

IT IS NOTIFIED for general information that His Excellency the President, after consultation with the Prime Minister and the Leader of the Opposition, in exercise of the power vested in him by section 4(4) of the Integrity in Public Life Act, 2000, has been pleased to appoint MR. VINDAR RABINDRANATH DEAN-MAHARAJ as a Member of the Integrity Commission, until the 23rd August, 2009.

H. HEMNATH
Secretary to His Excellency the President

1st September, 2006.

1604—*Continued*

REPUBLIC OF TRINIDAD AND TOBAGO

Policy and Procedural Guidelines for NETWORK SECURITY & ACCESS CONTROL

MINISTRY OF PUBLIC ADMINISTRATION AND INFORMATION

Version 1.0
April 21, 2006

1604—*Continued*

1.1 Policy Name

This policy may be referred to as the **Network Security and Access Control Policy and Procedural Guidelines.**

1.2 Target Audience

This policy is intended for all Government of Trinidad and Tobago (GoRTT) employees, consultants, public service agencies requiring Internet services and utilizing the IT infrastructure, computer resources and software applications provided by GoRTT.

1.3 Policy Purpose

Access to GoRTT computer systems and software applications should be managed and controlled without exposing GoRTT to the compromise of its assets, unacceptable disruption or risks. It is also crucial that all levels of the government's IT infrastructure remain secure, since this infrastructure will support all government applications. Access control includes *physical* and *logical* considerations, with both methods requiring the appropriate controls relevant to the risk factors associated with the actual, systems, equipment or information.

In response to these issues of network security and access control, this policy was developed.

1.4 Policy Maintenance History

This Policy is a dynamic document and may be revised and updated as required. Revisions are to be tracked and detailed below.

Date	Change details	Author	Version
04-Nov-04	Initial Draft	MPAI	0.0.1
12-Dec-04	Published for GoRTT approval	MPAI	0.1.0
19-Jan-05	Policy Revision inclusive of comments and recommendations	MPAI	0.2.0
23-Sept-05	Minor corrections to prepare document for presentation to Cabinet for approval	MPAI	0.3.0
10-Oct-05	Updated to include comments from PS	MPAI	0.4.0
31-Oct-05	Updated to include comments from DPS	MPAI	1.0.0

1.5 Policy Summary

This document provides broad policy statements in respect of Network Security and Access Controls, and procedural guidelines in the following areas:

a) Logical Access Control;
b) Physical Access Control;

1604—*Continued*

c) Network Security;
d) Cabling; and
e) Portable Devices.

1.6 Compliance

Everyone within GoRTT and those 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, including friends and relatives, who do not have a need to know the information in order to meet their professional responsibilities to GoRTT.

GoRTT will ensure that use of company computing and network resources does not infringe criminal or civil laws and international standards, 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 misuse of GoRTT resources. Violations of this policy may lead to appropriate disciplinary action in accordance with governing Human Resource policies.

1.7 Administration

Policy Ownership

This policy document is prepared and maintained by the Ministry with responsibility for overseeing and managing GoRTT's Information and Communications Technology (ICT) function. It is the responsibility of this Ministry to implement and enforce this Policy to ensure compliance.

The policy will be reviewed to ensure that it is addressing current threats, vulnerabilities, risks 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.

General Responsibilities

Ministry responsible for overseeing and managing GoRTT's ICT function

Responsible for endorsing and supporting GoRTT's policies in respect of Information Security, for ensuring that information security retains a high profile within GoRTT at the Ministry level and for guaranteeing that appropriate budget and personnel resources are available for the ongoing development, implementation and review of appropriate policy implementation. This Ministry must approve major initiatives aimed at enhancing information security.

1604—*Continued*

Employees and Consultants

Information security is not simply an ongoing managerial task - it is also the responsibility of each and every individual. As such, all 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 information security policies, procedures and responsibilities;
- Approve appropriate computer and resource access;
- Review, evaluate and respond to all security violations reported by employees and consultants and take appropriate action;
- Communicate with the appropriate public service agencies on employee and consultant departures, arrivals and changes which affect computer access;
- Ensure security procedures are in place to protect information assets under their control. Such procedures would include physical access control and virus protection for workstations, applications, local area networks, etc.; and
- Inform System Administrators on changes to access rights to data and systems, including the removal or creation of specific individual access rights.

Information Owners

'Information Owners' for all computer systems and information will be established. Information owners are responsible for their information and, in particular, for its classification according to the GoRTT Data Classification and Control Policy.

Public Service Agency IT Management and Technical Staff

Responsible for the implementation of GoRTT's policies in respect of Information Security within their Ministry and ensuring employees and consultants using the computer and network systems comply with this policy and report and violations to the Ministry with responsibility for overseeing and managing GoRTT's ICT function, or any agency it may designate to monitor this function.

1.8 Associated Documents

This policy and any subsequent guidelines, standards and procedures will be developed in accordance with the laws of the Republic of Trinidad and Tobago, more specifically, but nor limited to:

- The Computer Misuse Act;
- Freedom of Information Act;
- Integrity in Public Life Act;
- Data Protection Bill (not yet submitted to Parliament);
- Electronic Transaction Bill (not yet submitted to Parliament); and
- Other international standards, e.g. ISO ANSI.

1604—*Continued*

This policy is also linked to the following policies:

- Remote Access Policy; and
- Network Maintenance Policy.

1.9 Policy Statements

It is crucial for the effectiveness and success of an information security program that all levels of GoRTT's IT infrastructure be secure. System users are to be granted the minimum level of *physical* and *logical* access necessary for them to perform their work. Physical access controls should limit who has access to the equipment and logical access controls should reduce the risk of accidental or malicious disclosure, and modification or deletion of information.

Logical access controls should be specified for all systems and, wherever possible, enforced through appropriate operating systems and application configurations.

Computer systems and network components should be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage.

Since it is GoRTT's IT infrastructure on which all government applications will be supported, the security controls of the network devices supporting these business applications must establish a secure technical foundation. The Ministry with responsibility for overseeing and managing GoRTT's ICT function must approve the establishment and alteration of all external network connections with due consideration of the business needs and effect of network security on the Communications Backbone.

Data that is transmitted over GoRTT's IT infrastructure should not be altered in an unauthorized manner as a result of that transmission. GoRTT's IT infrastructure users should have a reasonable expectation that information which is being sent using the IT services is received at the intended destination in an unmodified state.

The functionality of network devices should be limited to that necessary to meet defined and approved network performance and security requirements.

1.9.1 Logical Access Control

Authentication

All access to GoRTT computer systems and network resources must be protected by an approved authentication mechanism.

1. Only authorized employees and consultants are allowed to access GoRTT resources.

1604—*Continued*

2. A valid, unique and non-generic User ID and password should be required for all system and network access (including intermittently connected computers).
3. User ID's should follow a standard naming convention, which facilitates the independent identification of the owner. This Naming Convention must be consistent with any future GoRTT document on Network Security Technical Guidelines.
4. A segregated privileged User ID for system administrative purposes must be identifiable to an individual user. Therefore, employees and consultants requiring privileged access capabilities must have two separate User IDs - one for regular access and one for privileged access.
5. Users are responsible for all activities performed with their personal User IDs. User IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their User IDs.
6. Privileged / administrator-level passwords and security device passwords should follow an enforced secure format e.g. 8 alphanumeric characters including at least 2 numeric characters.
7. User passwords should not be recorded or written down in such a way that an unauthorized person might discover them. Passwords must not be shared under any circumstances. Doing so exposes the authorized user to take responsibility for the actions of the other party using the password.
8. All user-specified passwords must be difficult to guess. Common character sequences "12345" and "abcd" should not be used. Passwords must therefore contain at least one alphabetic and one non-alphabetic character (numbers and punctuation).
9. All passwords must have **AT LEAST** 5 alphanumeric characters.
10. Any initial password provided to a new user must be valid only for the user's first on-line session. At that time, the user must be forced to choose another password before any other work can be done.
11. All users must be automatically forced to change their passwords at least once every sixty (60) days.
12. To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three (3) unsuccessful login attempts the user account must be disabled. This should only be re-activated once an employee / consultant can prove their identity to a System Administrator.
13. Trusted automated authentication, which requires no login with passwords, should not be allowed.

1604—*Continued*

14. Other than minimal prompts for User ID, password information and standard disclaimer information, no other information is to be displayed prior to logon.
15. The full name of the employee / consultant must be entered within the User Properties or Identification pages to correspond with the User ID.
16. Privileged or administrator-level passwords should be recorded and held under secure conditions by a nominated Ministry IT Manager, with proper backup and recovery procedures in place.
17. All vendor-supplied default passwords must be changed before any computer system is used by GoRTT

Access Privileges

1. All initial access granted to employees and consultants, and all changes to this access, should be authorized by the delegated Ministry's IT officer and/or senior Administrative Officer.
2. There should be a formal documented procedure for all requests for access.
3. Access request details should contain adequate information for the Administrative Officer and System Administrator to grant access and privilege levels accordingly.
4. Security requirements should be defined for each GoRTT business application and associated access rights and information classification should be documented.

Access Administration

1. System Administrators and IT Managers should be notified of employee and consultant arrivals, terminations and transfers before they occur, using a defined process.
2. Inactive logon User IDs should be monitored and disabled from the user authorization profile after 90 days of inactivity.
3. All emergency/temporary access should first be approved by a public service agency Manager and then usage should be monitored.
4. All activity using administrative accounts must be logged and monitored.
5. User access rights should be reviewed at least every 6 months. In cases where a user has privileged access rights, these rights should be reviewed every 3 months.
6. The system security software should be set to automatically disable temporary user accounts on a specified date.
7. User screens should be locked after 5 minutes of inactivity.

1604—*Continued*

Housekeeping and Audit

1. Detailed logs of all security events and sensitive transactions should be maintained. These should include, but not be limited to:

   - All unsuccessful login attempts;
   - All attempts to login using a privileged User ID;
   - Sensitive files and directories as defined by the Information Owner; and
   - Any access by developers to the production environment.

2. A formal audit of application controls will take place on the following basis:

   - High Risk Applications – Quarterly by the public service agency's IT Management and the Ministry with responsibility for overseeing and managing GoRTT's ICT function;
   - Medium Risk applications – Annually by the public service agency's IT Management; and
   - Low Risk Applications – Formal audits to take place periodically at the discretion of the Ministry with responsibility for overseeing and managing GoRTT's ICT function.

3. Significant findings or weaknesses identified from these audits must be mitigated in a timely manner by the public service agency's IT Management and the Information Owner.

1.9.2 Physical Access Control

1. All GoRTT owned systems and network components should be permanently and uniquely marked as GoRTT owned assets.

2. Network server systems and all storage media are to be physically protected from unauthorized access by at least one level of an approved physical access control mechanism. Secure facilities should be clearly defined and access to such facilities should be restricted to authorized employees and consultants only.

3. Servers and communication facilities should be housed in dedicated secure accommodations with access restricted to designated and appropriately qualified or contracted personnel working on behalf of the Information Owner.

4. GoRTT employees, consultants and visitors to secure facilities should wear visible identification while onsite.

1604—*Continued*

5. Critical GoRTT computer systems and network components should be located and operated within a managed security perimeter inside GoRTT facilities or trusted third party premises equipped with environmental monitoring controls.

6. Critical GoRTT computer systems and network components should be positioned away from potential hazards, including over-head water and heating systems, pipes and flammable materials.

7. To minimize theft and water damage, computer and communications facilities should not be located on the ground floors of buildings. To further minimize water damage, rest room facilities should not be located directly above these systems. Where possible, raised flooring should be used.

8. Critical GoRTT computer systems and network components should be protected by a filtered power supply and other appropriate environmental controls, and, if essential to business critical operations, covered by an uninterruptible power supply (UPS).

9. Security should be exercised over employees, consultants and visitor access to, and activities within, areas that maintain GoRTT business critical and significant GoRTT computer systems and network components.

10. Tours of major computer and communications facilities must be strictly controlled.

11. Computer equipment (PCs, LAN servers, etc.) should not be relocated without the prior approval of the IT Manager and/or senior Administrative Officer.

1.9.3 Network Security

1. Access to all network devices must follow approved authentication mechanisms.

2. Networks must be designed in conformance with GoRTT's established technical standards as they are developed or adopted. Network configurations must be accurately documented.

3. Network software should have the latest certified vendor software patches installed. Final configurations should ensure that device software is free of CERT® (Computer Emergency Response Team) advisories and known vendor vulnerabilities.

1604—*Continued*

4. Network devices should follow authorized backup and disaster recovery procedures. Backup media should be read-only and stored in a physically secured area accessible by authorized personnel only.

5. Access to software documentation and data storage should be restricted to employees, consultants and agents who need such access to perform assigned work duties.

6. Remote access administration to internal network components for support services should be authorized via the public service agency's remote access approval process. Please view the *Remote Access Policy*.

7. The operating system contained within network devices must be configured such that it precludes the opportunity for users or hackers to maliciously gain access to the device in order to reconfigure it.

1.9.4 Cabling

Network cabling should be clearly labelled to detail the following:

- Cables purpose; and
- Terminating switch port numbers.

Network cabling primarily carrying data classified as sensitive should be colour coded and properly labelled. The cable should be a different colour to the standard cabling, e.g. red as opposed to blue.

Network cabling, which is identified as primarily carrying data classified as sensitive, should be protected and controlled.

1.9.5 Portable Devices

1. Employees and consultants with portables, laptops, notebooks, palmtops and other transportable computers containing restricted or confidential information must not leave these computers unattended.

2. When traveling, employees and consultants with transportable computers containing restricted or confidential information must retain possession of these computers at all times.

3. Restricted or confidential information on off-line storage media, e.g. CD-ROM, diskettes, magnetic tape, USB keys, flash drives, memory sticks and removable storage devices must be adequately protected.

4. Refer to the *Remote Access Policy* for more details.

1604—*Continued*

2.0 Glossary or Terms

For ease of use and overall understanding of the technical terms of this Policy and others relative to this one, a glossary or terms is provided.

1	Unauthorized use	The use of GoRTT's computer and ICT infrastructure without the explicit consent of GoRTT or it's duly appointed agent(s).
2	Interception	The monitoring and/or recording of any aspects of content of electronic messages communicated via GoRTT's ICT networks.
3	Internet	The International Network of Networks that is a collection of hundreds of thousands of private and public networks.
4	Confidential or Sensitive Information	Classified data and/or facts which may not be disclosed without the explicit consent of GoRTT.
5	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.
6	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.
7	Infrastructure	The structured arrangement of physical components that define a communications network including cabling, routers, switches and computers.
8	Online	Being connected to the Internet via the World Wide Web.
9	Connectivity	A measure of how well computers and computer-based devices communicate and share information with one another without human intervention.
10	Software	The detailed instructions that control the operation of a computer system.

1604—*Continued*

11	Software Licenses	An agreement or legal document between the manufacturer (design and development) of the software and the purchaser with reference to the rules and regulations of use.
12	Computer-based information	Information that is stored in databases on computers (PCs, servers, etc.)
13	Computer Applications	Computer programmes written for a specific application to perform functions specified by end-users.
14	Network	A series of points/nodes connected by communication circuits.
15	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.
16	Security Violations	The infringement, abuse or breach of the rules and regulations with reference to computer systems accessibility and usage.
17	ICT (Information and Communications Technology)	The integration of telecommunications tools, devices and systems for communicating information and managing information across the globe.
18	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.
19	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.
20	Encryption	The coding and scrambling of messages to prevent their being read or accessed without authorized.

1604—*Continued*

21	Hacking	The act of gaining unauthorized entry/access to a computer network for profit, criminal mischief or personal pleasure.
22	Logical Access	Entry to computer / network systems via the appropriate "soft" mechanisms such as authentication through use of unique user names and passwords.
23	Physical Access	Entry via secured facilities to the actual tangible components of the computer / networking systems.
24	Segregated Privileged User ID	A user's identification code that is unique, separate and apart from other user's identification codes. Usually this code is assigned to the System's Administrator.
25	Inactive Logon User ID	A user's identification code that is used to gain access to a computer system that has become inactive after a prescribed period of time.
26	Terminating Switch Port Numbers	Numerical labels given or assigned to ports (points of entry and exit) of terminating switches.

1604—*Continued*

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

1604—*Continued*

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;

1604—*Continued*

b) To ensure accountability for the actions performed by each user, consistently 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.

1604—*Continued*

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.

1604—*Continued*

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;

1604—*Continued*

- 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.

1604—*Continued*

- 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.

1604—*Continued*

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;

1604—*Continued*

- 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*" 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.

1604—*Continued*

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.

1604—*Continued*

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.

1604—*Continued*

REPUBLIC OF TRINIDAD AND TOBAGO

Policy and Procedural Guidelines for
E-MAIL AND INTERNET USAGE

MINISTRY OF PUBLIC ADMINISTRATION AND INFORMATION

Version 1.0
April 21, 2006

1604—*Continued*

1.1 Policy Name

This policy may be referred to as the **E-mail and Internet Usage Policy and Procedural Guidelines.**

1.2 Target Audience

This policy is intended for all Government of the Republic of Trinidad and Tobago (GoRTT) employees, Information and Communications Technology (ICT) managers and consultants utilizing Internet and E-mail services which require the ICT infrastructure, computer resources and software applications provided either directly or remotely by GoRTT.

1.3 Policy Purpose

Information is a critical asset for operational business functions and service delivery of 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 and confidentiality of this asset.

The wide array of resources, services, and connectivity available via the Internet and E-mail expose GoRTT to a variety of security and confidentiality risks, which include but are not limited to the following:

(a) Access to GoRTT's ICT networks and the information contained therein by unauthorized users;
(b) The introduction of non-standard and/or malicious software into GoRTT's ICT environment; and
(c) The interception or monitoring of proprietary and/or confidential information communicated over the Internet or E-mail;

This policy was developed in response to these, and other potential E-mail and Internet risks.

1604—*Continued*

1.4 Policy Maintenance History

This policy is a dynamic document and may be revised and updated as required. Revisions are to be tracked and detailed below.

Date	Change details	Author	Version
20-Nov-04	Initial Draft	MPAI	0.0.1
12-Dec-04	Published for GoRTT approval	MPAI	0.1.0
19-Jan-05	Policy Revision inclusive of comments and recommendations	MPAI	0.2.0
23-Sept-05	Minor corrections to prepare document for presentation to Cabinet for approval	MPAI	0.3.0
06-Oct-05	Updated to include comments from PS	MPAI	0.4.0
31-Oct-05	Updated to include review comments from DPS	MPAI	1.0.0

1.5 Policy Summary

Internet and E-mail connectivity are essential business tools for GoRTT in accordance with Trinidad and Tobago's National ICT Strategy. The objective of this policy is thus to minimize the risks arising from the use of the Internet and E-mail services without unduly hindering GoRTT's ability to deliver quality services internally and to the public.

In order to satisfy this policy's objective, GoRTT must establish controls for use of Internet and E-mail services. This policy will address the following objectives:

1. To standardize Internet and E-mail services provided to employees and consultants in order for them to have the means and tools necessary to fulfill their tasks and perform their job function activities in an effective and efficient manner;
2. To ensure that each user is accountable for their actions in use of the GoRTT ICT services, and that their activities are consistent with GoRTT's expectations and comply with published policies; and
3. To protect GoRTT's data network resources from unauthorized access and abuse.

1.6 Compliance

All information created by employees and consultants in the course of their official duties, or information specifically developed for GoRTT, is the sole property of GoRTT. Additionally, any information which is residing within GoRTT's ICT infrastructure is also considered to be the sole property of GoRTT, with the exception of materials belonging to other entities for which GoRTT has usage permission (e.g. copyrighted materials).

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

1604—*Continued*

Employees and consultants must not disclose confidential and\or sensitive information to third parties, including relatives, friends and professional acquaintances.

GoRTT will monitor and ensure that the use of its computing and network resources does not infringe criminal or civil laws, regarding the storage or transmission of libelous, seditious, indecent or offensive material.

Employees and consultants must be aware that there are consequences for intentional misuse of GoRTT resources. Violations of this and other relevant policies may lead to disciplinary action, in accordance with governing Human Resource policies.

1.7 Administration

1.7.1 Policy Ownership

This policy document is prepared and maintained by the Ministry with responsibility for overseeing and managing GoRTT's Information and Communications Technology (ICT) functions. 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 threats, vulnerabilities, risks and the requirements of GoRTT. Any revisions or modifications to this policy must be approved by the Ministry referred to above. Questions concerning the policy and suggested revisions should be directed to this Ministry.

1.7.2 General Responsibilities

Ministry responsible for overseeing and managing GoRTT's ICT functions

Responsible for endorsing and supporting GoRTT's policies in respect of Information Security, for ensuring that information security retains a high profile within GoRTT at the Ministry level. The Ministry is also responsible for guaranteeing that appropriate budget and personnel resources are available for the ongoing development, implementation and review of appropriate policies. The Ministry will approve major initiatives aimed at enhancing information security.

Employees and Consultants

Information security is not simply an ongoing managerial task - it is also the responsibility of each and every individual. As such, all employees and consultants are expected to respect this policy in spirit and comply with the statements contained herein.

1604—*Continued*

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 information security policies, procedures and responsibilities;
- Approve appropriate computer and resource access;
- Review, evaluate and respond to all security violations reported by employees and consultants and take appropriate action;
- Communicate to appropriate public service agencies when employee or consultant departures, arrivals and changes affect computer access;
- Ensure security procedures are in place to protect the information assets under their control. Such procedures would include physical access control and virus protection for workstations, applications, local area networks, etc.; and
- Inform System Administrators of changes to access rights to data and systems, including the removal or creation of specific individual's access rights.

Information Owners

GoRTT's computer systems and information which need protection must have a designated 'Information Owner'. Information Owners are responsible for the information under their control and, in particular, for its classification according to GoRTT's Data Classification and Control Policy.

Public Service Agency Information Technology (IT) Management and Technical Staff

Responsible for the implementation of GoRTT's policies in respect of Information Security within their Ministry and ensuring that employees and consultants who have access to, and use of, the computers and network systems of GoRTT comply with this and other relevant policies. The specific Ministry's Information Technology (IT) Management and Technical Staff are also responsible for the reporting of policy violations to the Ministry with responsibility for overseeing and managing GoRTT's ICT function, or any agency it may designate to monitor this function.

1.8 Policy Statements

Access to, and use of, the Internet and E-Mail services are tools provided to enable users to perform their job functions in an effective and efficient manner. The public service agencies' electronic information resources are to be used in a responsible manner consistent with the purposes for which they are intended.

The following procedural guidelines must be employed by public service agencies' use of e-mail and the Internet.

1604—*Continued*

1.8.1 E-mail

a. A public service agency's electronic mail system is to be used only for business purposes. All messages sent by electronic mail constitute government records. The public service agency reserves the right to access and disclose all messages sent via its electronic mail system, for any purpose, and specifically in accordance with the Freedom of Information Act of 2002. A public service agency therefore may also disclose electronic mail messages to law enforcement officials without prior notice to an employee or consultant, who may have sent or received these messages.

b. Employees or consultants must not use an electronic mail account assigned to another individual to either send or receive messages.

c. Users must not use profanity, obscenities, racist or derogatory remarks in electronic mail messages discussing employees, clients or customers. Such remarks, even when made in jest, may have legal implications such as libel and defamation of character.

d. Unless the information is encrypted, users must refrain from sending credit card numbers, passwords, and other sensitive data via electronic mail since the interception of this type of data by unscrupulous individuals can be unfavorable for the user.

e. Employees and consultants are prohibited from sending or forwarding, either manually or automatically, any messages via GoRTT's information systems that may reasonably be interpreted as defamatory, harassing or explicitly sexual. Employees and consultants are also prohibited from sending or forwarding, either manually or automatically, messages or images that would likely be offensive on the basis of race, ethnicity, gender, age, national origin, sexual orientation, religion, political beliefs or disability.

f. A systematic process for the recording, retention and destruction of electronic mail messages and accompanying logs must be developed with the following guidelines:
   - The decision to remove electronic mail is vested with the Information System Manager, or the most senior officer responsible for Information Technology (IT) functions in a public service agency;
   - Electronic logs archived after 90 days may be destroyed one year after being archived; and
   - Messages longer than 90 days old may be archived.

g. Electronic mail systems are not intended for the archival storage of important information. Information that is deemed important enough

1604—*Continued*

to be kept for future reference must be stored in another format, filed in accordance with the public service agency's registry function, and saved for as long as needed. Systems administrators should therefore periodically expunge stored electronic mail messages in accordance with guidelines given above.

h. E-mail attachments should observe the same formats in respect of official correspondence for specific purposes. If executable programs or other non-text messages must be sent, other methods of transmission such as FTP (File Transfer Protocol) should more appropriately be used.

i. It should be noted that although the Internet and E-mail are informal communications environments, the laws governing copyrights and patents are applicable. Employees and consultants should not transmit copyrighted materials without the written permission of the owner or the Copyright Organization of Trinidad and Tobago.

j. All E-mail messages should have the employee's / consultant's name attached with contact information detailed in the signature. The signature details should include the following minimum information:
   - Author's name;
   - Author's position within his or her agency;
   - Agency division and/or section; and
   - Agency address, telephone number and fax number.

k. Information of a sensitive nature that also constitutes non-public customer information should be delivered via another medium. If it is necessary to do so, employees and consultants should take reasonable steps to ensure that the information is delivered to the person who is authorized to receive and use it for a legitimate purpose.

l. At a minimum, all E-mail messages must be appended with the following disclaimer: "This message is intended only for the named recipient(s). If you are not the intended recipient(s) you are hereby notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited."

m. While electronic mail is provided to all employees, all other types of Internet access are reserved for those who have a demonstrated business need for such access. All access to the Internet therefore must be approved in advance and in writing by the relevant agency official.

n. Users must not advertise, promote, present or make statements about an agency's Internet services such as mailing lists, newsgroups, chat

1604—*Continued*

rooms or sessions, without prior approval from the relevant Communications department and/or senior administrative manager.

o. All software and files downloaded from the Internet must be checked with an authorized virus detection package. This screening must take place prior to being opened or examined via another program such as a word processing package.

p. E-mail systems should not be used for broadcast facilities to large numbers of employees for the purpose of sending common information (e.g. declaration of public holidays, pay dates, etc). It is recommended that such information be sent to bulletin boards.

q. The use of the agencies' workstations and/or ICT infrastructure for any illegal or criminal purpose that violates applicable laws, including, but not limited to, committing fraud, violating copyright law or software licenses is strictly prohibited;

1.8.2 Internet

The following scenarios illustrate unacceptable or inappropriate usage of the Internet:

a. Disrupting the intended use of the agency's Internet computers;

b. Damaging the integrity of computer-based information on the agency's Internet computers by attempting to install, delete or modify the agency's software, or attempting to install or run any programs that have not been installed by the agency;

c. Moving or changing the arrangement of the agency's computers and attached equipment;

d. Unauthorized downloading of software from the Internet onto the Ministries' computers or onto disks;

e. Attempting to gain unauthorized access to the resources of the agency's network or Internet computers;

f. Deliberately engaging in activities that result in the degradation of system performance across the agency's network;

g. Attempting to gain unauthorized access, including so-called "hacking," to the resources of other networks;

1604—*Continued*

h. Developing computer programs, which infiltrate a computer or computer system and/or damage or alter the software components of a local or remote computer or computer system;

i. Deliberately displaying and/or viewing obscene images;

j. Engaging in communications which are libelous or slanderous;

k. Unauthorized disclosure, use, and dissemination of personal information regarding minors, or otherwise compromising the privacy of any users;

l. Wasting of resources (staff time, equipment capacity, supplies) through such actions;

m. Using the Internet for illegal purposes;

n. Transmitting threatening, harassing or defamatory materials or messages;

o. Committing fraud;

p. Violating copyright law or software licenses;

q. Transmitting chain mail, broadcast letters, or junk mail of any type.

1.9 Associated Policies and Documents

- Network Security and Access Control Policy
- Remote Access Policy
- Data Classification and Control Policy
- Computer Misuse Act (2000)

1604—*Continued*

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	Internet	An electronic communications network that connects computer networks and organizational computer facilities around the world.
1	Unauthorized use	The use of GoRTT's computer and ICT infrastructure without the explicit consent of GoRTT or it's duly appointed agent/agents.
2	Interception	The monitoring and/or recording of any aspects of content of electronic messages communicated via GoRTT's ICT networks.
3	Confidential or Sensitive Information	Classified data and/or facts which may not be disclosed without the explicit consent of GoRTT.
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	Connectivity	A measure of how well computers and computer-based devices communicate and share information with one another without human intervention.

1604—*Continued*

9	Software	The detailed instructions that control the operation of a computer system.
10	Software Licenses	An agreement or legal document between the manufacturer (design and development) of the software and the purchaser with reference to the rules and regulations of use.
11	Computer-based information	Information that is stored in databases on computers (PCs, servers, etc.)
12	Computer Applications	Computer programmes written for a specific application to perform functions specified by end-users.
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	Security Violations	The infringement, abuse or breach of the rules and regulations with reference to computer systems accessibility and usage.
16	Physical Access	Entry via secured facilities to the actual tangible components of the computer / networking systems.
16	ICT (Information and Communications Technology)	The integration of telecommunications tools, devices and systems for communicating information and managing 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.

1604—*Continued*

19	Encryption	The coding and scrambling of messages to prevent their being read or accessed without authorization.
20	Hacking	The act of gaining unauthorized entry/access to a computer network for profit, criminal mischief or personal pleasure.

1605

GRANT OF CERTIFICATES OF REGISTRATION

(Citizenship of the Republic of Trinidad and Tobago Act, 1976)

Number	*Name*	*Date*
11633	SAVATRI RAMCHARITAR	16th August, 2006—(NS: 19/2/1 S. 14210)
11635	BERNADETTE CASSILA CASTLE	16th August, 2006—(NS: 19/2/1 S. 12735)
11636	CANDACE ONICA VANESSA AARON	16th August, 2006—(NS: 19/2/1 S. 14093)
11637	SHAMIROOL MOHAMMED	16th August, 2006—(NS: 19/2/1 S. 14290)
11639	ALMAIDER ALBERTHA POPE	16th August, 2006—(NS: 19/2/1 S. 14283)

J. BOUCAUD-BLAKE
Acting Permanent Secretary,
Ministry of National Security

1606

GRANT OF CERTIFICATE OF NATURALISATION

(Citizenship of the Republic of Trinidad and Tobago Act, 1976)

Number	*Name*	*Date*
730	XINGHUA ZHANG-LUM	16th August, 2006—(NS: 19/2/1 S. 772)

J. BOUCAUD-BLAKE
Acting Permanent Secretary,
Ministry of National Security

1607

GRANT OF CERTIFICATE OF CITIZENSHIP

CERTIFICATE OF CITIZENSHIP No. 65 granted under section 11(2) of the Citizenship of the Republic of Trinidad and Tobago Act, Chap. 1:50 of the Laws of Trinidad and Tobago has been issued to DILLON VANDIXCAW YEARWOOD.

J. BOUCAUD-BLAKE
Acting Permanent Secretary,
Ministry of National Security

16th August, 2006—Ref. (NS: 19/10/2 S. 91).

1608

RENUNCIATIONS OF TRINIDAD AND TOBAGO CITIZENSHIP

IAN ANTHONY OWEN BROWNE JR. who was born in the United States of America on 1st November, 1976, and is a citizen of Trinidad and Tobago by descent has renounced his Citizenship of the Republic of Trinidad and Tobago.

This has been recorded at the Ministry of National Security.

V. BELGROVE
Permanent Secretary,
Ministry of National Security

2nd August, 2006—Ref. (NS/C&I: 19/4/1 Vol. XVII).

1609

JUDY MELVA PHILLIP who was born in Trinidad and Tobago on 18th November, 1962, has renounced her Citizenship of the Republic of Trinidad and Tobago.

This has been recorded at the Ministry of National Security.

J. BOUCAUD-BLAKE
Acting Permanent Secretary,
Ministry of National Security

11th August, 2006—Ref. (NS/C&I: 19/4/1 Vol. XVII).

1610

LICENSING SESSIONS

CHAGUANAS

RETURN of Applications for Licensing Committee's Certificates for Licences to sell Intoxicating Liquor in the Magisterial District of Caroni, under the provisions of the Liquor Licences Act, Chap. 84:10, to be considered at the Licensing Session will be held at the Chaguanas Magistrate's Court on THURSDAY THE 14TH DAY OF SEPTEMBER, 2006 at the hour of 9.00 o'clock in the forenoon.

Name of Applicant	*Occupation*	*Abode of Applicant*	*Premises where Situate*	*Term of Licence*
Spirit Retailer's				
Steve Maharaj	Unemployed ...	No. 1 Leekham Road Mamoral No. 2 Mamoral	No. 1 Leekham Road Mamoral No. 2 Mamoral	From 1st October, 2006 31st March, 2007
Raghubar Ramsamaroo ...	Self-employed	57, Rodney Road Endeavour Village Chaguanas	57, Rodney Road Endeavour Village Chaguanas	do.

Dated this 25th day of August, 2006 at the Chaguanas Magistrate's Court.

T. RAMLAL
Secretary, Licensing Committee, Caroni

1611

SANGRE GRANDE

APPLICATIONS for Licensing Committee's Certificates for New Licences in the Licensing District of North-Eastern Counties (St. Andrew and St. David) under the provisions of the Liquor Licences Act, Chap. 84:10 will be considered at a Licensing Session to be held at the Sangre Grande Magistrate's Court on WEDNESDAY THE 13TH DAY OF SEPTEMBER, 2006 at 9.00 o'clock in the forenoon.

Name of Applicant	*Occupation*	*Abode of Applicant*	*Premises where Situate*	*Term of Licence*
Spirit Retailer's				
Steve Jules	Proprietor ...	No. 2 Crescent Drive Mausica Road d'Abadie	Eastern Main Road Valencia Junction	From 1st October, 2006 31st March, 2007
Aftab Mohammed	Proprietor ...	$3^3/_4$ Mile Mark, Vega De Oropouche Toco Road Sangre Grande	$3^3/_4$ Mile Mark, Vega De Oropouche Toco Main Road Sangre Grande	do.
Christine George-Huggins ...	Labourer ...	North Manzanilla No. 4	North Manzanilla No. 4	do.
Naresh Persad	Proprietor ...	5A, Boodooville Circular Road Sangre Grande	5A, Boodooville Circular Road Sangre Grande	do.
Spirit Grocer's				
Pramdath Jaghoo	Proprietor ...	$12^3/_4$ Mile Mark Cumuto Main Road Coryal	$12^3/_4$ Mile Mark Cumuto Main Road Coryal	do.
Seepersad Maharaj	Proprietor ...	Light Pole No. 61 Oropouche Road Sangre Grande	Valencia Central Market Alexander Road Valencia	do.
Nalini Motilal	Proprietor ...	Light Pole No. 15 Toco Road Sangre Grande	Light Pole No. 15 Toco Road Sangre Grande	do.

Dated this 29th day of August, 2006 at the Sangre Grande Magistrate's Court.

R. SADHU
Secretary, Licensing Committee, North-Eastern Counties

1612

REPUBLIC OF TRINIDAD & TOBAGO

PRE-QUALIFICATION FOR CONSULTANCY SERVICES

FOOD AND BEVERAGES INDUSTRY

Pre-qualification applications are invited from suitably qualified professionals and consultancy firms who wish to be placed on the shortlist of experts for specific issues, reports, workshops and related matters for the one or more projects included in the components listed below.

These components form part of the work programme for the development and increased competitiveness and growth of the domestic Food and Beverage Industry. Shortlisted consultants would be required to:

- ***Plan, execute and evaluate workshops for stakeholders in the domestic Food and Beverage Industry***
- ***Provide reports, and develop strategies for improving the Food and Beverage Sector in the areas mentioned below***
- ***Report to the Food and Beverage Industry Development Committee as required to provide an update on the progress of their activities***

Areas of Specialty required:

Component	Area of Specialty	Subcomponent Projects
1	Market Development Capability	Developing workshops and training modules to increase market intelligence capability among firms
2	Increasing Competitiveness among Small and Medium Enterprises	Developing workshops and training modules in production excellence, supply chain management and lean manufacturing Increasing Research, Development and Innovation Human Resource Development and training
3	Developing Linkages	Deepening linkages and creating cooperative clusters among stakeholders in the industry, which include but is not limited to primary producers, other suppliers, processors and higher value-added services

Envelopes must be deposited in the white Tenders Box located in the lobby at Level 15 of the Ministry's Office at Riverside Plaza on or before **Friday 18th August 2006 at 1:00 pm.**

Late applications will not be accepted under any circumstances.

Pre-Qualification Questionnaires:
Visit www.tradeind.gov.tt/ FBIDC.HTM or collect them at the Ministry of Trade and Industry, Level 15 Riverside Plaza, Port-of-Spain.

For Further Information:
Contact: Mr. Richard Ramsawak
Industry Specialist
Tel: (868) 625-4792
Fax: (868) 624-9594
or via e-mail: rramsawak@tradeind.govt.tt

Submission of Questionnaires:
Completed questionnaires should be enclosed in sealed envelopes clearly marked "Pre-qualification for Consultancy Services for the Food and Beverage Industry" and addressed to:

The Chairman
Ministerial Tenders Committee
Ministry of Trade and Industry
Level 15 Riverside Plaza
Port-of-Spain

mti
MINISTRY OF TRADE AND INDUSTRY