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

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;

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.

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.

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.

2. A valid, unique and non-generic UserID and password should be required for all system and network access (including intermittently connected computers).
3. UserID'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 UserID for system administrative purposes must be identifiable to an individual user. Therefore, employees and consultants requiring privileged access capabilities must have two separate UserIDs - one for regular access and one for privileged access.
5. Users are responsible for all activities performed with their personal UserIDs. UserIDs 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 UserIDs.
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.

14. Other than minimal prompts for UserID, 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 UserID.
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 UserIDs 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.

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 UserID;
    - 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.

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.

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.

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.
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.

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.