



Policy on

Protection of Personal Privacy and Data Security

Trinidad & Tobago Government Internet (Web) Presences

Version 1.0

December 2006

Table of Contents.

1.	POLICY NAME	2
2.	TARGET AUDIENCE.....	2
3.	SCOPE OF APPLICATION	2
4.	POLICY PURPOSE.....	2
5.	POLICY OBJECTIVES.....	2
6.	POLICY CONTEXT	3
7.	POLICY MAINTENANCE HISTORY	3
8.	INTRODUCTION.....	5
9.	POLICY PRESCRIPTIONS	9
9.1	Requirements of TTGOV web sites include:	9
9.2	Recommended standards for TTGOV web sites include:	10
10.	REFERENCES.....	12

1. Policy Name

Policy on Protection of Personal Privacy and Data Security for Trinidad and Tobago Government Internet (Web) Presences.

2. Target Audience

This Policy is targeted to the Permanent Secretaries, Heads of Departments, Managers, Legal Services Branches, Operational Specialists, Communication Specialists, IT Professionals, Records Managers, and any persons responsible for the design, development, maintenance and approval of content and business services provided on or through web sites and portals for Ministries and agencies of the Government of Trinidad and Tobago (TTGOV)..

3. Scope of Application

This Policy is applicable to Internet web sites and portals of:

- (i) All Government Ministries, agencies, departments and the Tobago House of Assembly,
- (ii) All statutory authorities.

The Ministry with the responsibility for the Enterprise Full Service e-Government Portal (e-Government Portal) will administer the requirements of this Policy. Any requests for exemptions or exceptions to this Policy should be forwarded to the Ministry with responsibility for the e-Government Portal in writing and the granting of such exemptions or exceptions shall be subject to Cabinet approval.

Private or state-owned companies are not covered by this Policy. It should be noted, however, that this Policy sets out protection of privacy and security practices relating to web-based activity that should be viewed as "best practices" suitable for adoption by these companies.

4. Policy Purpose

The purpose of this Policy is:

- 1) to ensure compliance with the provisions of the Data Protection Policy (approved by Cabinet, January 2006); and
- 2) to build citizens' trust in TTGOV web sites and the e-Government Portal and, in particular, heighten individual confidence that personal information will be treated according to modern, internationally agreed standards regarding the collection, use, retention and disposal of such information.

5. Policy Objectives

The following standards for the protection of personal privacy are intended to ensure that:

- The collection and handling of personal data through TTGOV web sites are done in a manner consistent with Data Protection Principles; and
- Electronic records created by interactions with TTGOV web sites are managed (i.e., retained, authenticated, stored and disposed of) in accordance with an established and recognized protocol.

In order to achieve these objectives, the Government of Trinidad and Tobago will:

- Develop Privacy Impact Assessments (PIAs) for each TTGOV web site;
- Review business processes associated with TTGOV web sites to ensure compliance with the Data Protection Principles;
- Institute the necessary processes and procedure that ensure compliance with the Data Protection Principles; and
- Place a Privacy Statement on each TTGOV web site.

Subsequent policies will elaborate and complement these standards in the areas of:

- (i) Content Management; and
- (ii) Authentication.

6. Policy Context

This Policy on Protection of Personal Privacy shall be consistent with the Data Protection Policy and any subsequent legislation dealing with the protection of personal privacy and may be amended from time to time as the need arises.

Legislation and policy guidelines relevant to the Policy on Protection of Personal Privacy and Data Security include:

Constitution of the Republic of Trinidad and Tobago
Government Communications Policy
Civil Service Act, No. 45 of 1979
Freedom of Information Act, No. 26 of 1999, as amended
Tobago House of Assembly Act, No. 37 of 1980
Data Protection Policy and Commentary
Electronic Transactions Policy and Commentary
Policy on Content and Presentation Design Standards
Policy on Network Security and Access Control
Policy on Risk Management (Draft)
Policy on Electronic Records Management (Draft)
Web Content Management Policy (forthcoming)

7. Policy Maintenance History

Date	Change Details	Author	Version
Dec 13 06	Final review after consultation	ICT Policy	1.0

The ICT Policy and Stakeholder Engagement Unit of the ICT Division, Ministry of Public Administration and Information is responsible for this document.

Comments should be sent to:

National Chief Information Officer

ICT Division

Ministry of Public Administration and Information

Level 3, Lord Harris Court,

52 Pembroke Street,

Port of Spain,

Trinidad & Tobago

e-mail: fastforward@gov.tt

Tel: + 1 868 627 9642

Fax: +1 868 624 8001

The Effective Date of this Policy is the date of approval by the Cabinet.

For existing web presences as of September 1, 2006, compliance shall be no later than November 1, 2007

8. Introduction

Pursuant to objectives outlined in the National ICT Strategy, **fastforward**, the Government of Trinidad and Tobago is developing an Enterprise Full Service e-Government Portal for the dissemination of government information and provision of government services. This e-Government Portal is intended to provide a single point of entry for end user access to government information and services, whether delivered through electronic means or other channels.

The e-Government Portal and other **fastforward** initiatives provide unique opportunities for communication with citizens and Internet users throughout the world. It also provides new opportunities for the provision of services and creates the potential for new forms of services, including improved and better targeted interactions with citizens, more extensive consultations with stakeholders involved with new policies and government activities, and enhanced democratic structures.

Trust is a critical component in the success of TTGOV web sites, the e-Government Portal and e-commerce generally: citizens must be able to trust how their government handles their personal information and protects their privacy. Privacy is the "right of the individual to be protected against intrusion into his or her personal life or affairs...by direct physical means or by publication of information."¹ Privacy has long been understood to have a value in a civil society and is the reasonable expectation of every individual. The Universal Declaration of Human Rights 1948 (article 12) clearly establishes the right to privacy as a fundamental human right.² This right was subsequently enshrined in the Constitution of Trinidad and Tobago as Chapter 1, section 4(c), which recognises the right of the individual to respect for his private and family life. Increasing use of Computers and information technology, however, raises new issues regarding data about individuals and potential threats to personal privacy. For example, computers:

- facilitate the collection and maintenance of extensive record systems and the retention of data on those systems;
- make data easily and quickly accessible from many distant points;
- facilitate the speedy transfer of data from one information system to another and one jurisdiction to another; and
- make it possible for data to be combined in ways that might not be otherwise practicable and yet yields entirely new and in-depth information about an individual.

As a result of the multi-faceted use of personal data in computing systems, citizens in many countries are becoming increasingly concerned about protection of their personal information, whether it is held by a government or by private sector firms. Some polls, in fact, reveal that citizens are even more reluctant to submit personal information to government web sites than to private sites. The general concern about privacy of personal information is one of most common reasons why citizens avoid using government web sites and trust must continually be earned for e-government services to reach their full potential. This can be done through the meticulous use of proper data protection policies.

Responding to citizen concerns about the protection of their personal information, the Government of Trinidad and Tobago developed a Data Protection Policy, which was approved

¹ United Kingdom, Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, ("Calcutt Committee"), 1990, Cmnd. 1102, London: HMSO, page 7.

² Article 12 states, "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks."

by Cabinet in January 2006. This Policy sets out Data Protection Principles, as well as rules for the collection and handling of personal information. Legislation consistent with this Policy is being developed and will be introduced into Parliament. This Policy is mandatory for TTGOV Ministries, departments and agencies and represents “best practices” for the private sector and quasi-governmental organisations. The Policy is consistent with international standards and practices, including those adopted in the European Union and other developed countries. Like other modern data protection legislation, the Data Protection Policy is based on data protection principles developed by the Organisation for Economic Co-operation and Development. The Policy’s Data Protection Principles are the following:

- Principle 1: Accountability. An organisation is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organisation's compliance with the following [data protection] principles.
- Principle 2: Identifying Purposes. The purposes for which personal information is collected shall be identified by the organisation at or before the time the information is collected.
- Principle 3: Consent. The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
- Principle 4: Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organisation. Information shall be collected by fair and lawful means.
- Principle 5: Limiting Use, Disclosure and Retention. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
- Principle 6: Accuracy. Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
- Principle 7: Safeguards. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
- Principle 8: Openness. An organisation shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- Principle 9: Individual Access. Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- Principle 10: Challenging Compliance. An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organisation's compliance.

When enacted as legislation, the Data Protection Policy will create an Office of the Data Commissioner, who will have be responsible for ensuring and promoting compliance with the legislation. In the meantime, however, each TTGOV Ministry, department and agency must put in place the processes and procedures necessary for compliance with the Policy, as approved by Cabinet. In particular, they must ensure that their web sites are compliant with the Data Protection Principles and that all personal information collected in the course

of web-based transactions is treated in a manner consistent with the protections provided by the Data Protection Policy. This Policy is intended to provide further guidance on the protection of personal privacy in e-government generally and specifically related to web sites and web-based transactions.

Two main techniques are used to further the protection of personal privacy on TTGOV web sites:

- Privacy Impact Assessments (PIAs); and
- Privacy Statements.

A Privacy Impact Assessment is a specialized type of risk assessment that examines the potential impact that a program or activity may have on personal privacy. It examines the need for and the type of personal information being collected, identifies the risks of violation of the Data Protection Principles (e.g., the sensitivity of the data, the need for data sharing, the likelihood of secondary use of the data), and identifies the procedures, technologies and steps that may be taken to mitigate risks and enhance data protection.

While the Data Protection Policy is aimed at the protection of personal information being held, created or collected by each TTGOV ministry, department and agency generally, this Policy deals more specifically with personal information being collected on or through TTGOV web sites. This information will be linked to the business needs of various government programs and services, which must in turn meet the requirements of the Data Protection Policy. This Policy, therefore, exists within the context and requirements of the approved Data Protection Policy. It is, however, more focused and is aimed at ensuring that citizens know that they can trust government when they are asked to provide personal information to government over the Internet.

Protection of personal privacy on the Internet raises unique concerns.³ The user is effectively alone in interacting with the web site so the web site must draw the user's attention to privacy-related information. That information must be clear, unequivocal and obvious. A web site can collect information covertly (e.g., through cookies or web beacons⁴) as well as overtly (e.g., through filling out an online form). Thus, information collection may be invisible to the user. TTGOV web sites have an obligation to take the lead and provide a model in Trinidad and Tobago for the protection of personal privacy on the Internet. This must be a concern at every stage, from the design and development of web sites and the adaptation of existing government programs, to online service delivery, to the notification of users of their rights and protections, to the maintenance of a secure environment for the collection, use, storage and disposal of personal information held by government. This Policy establishes rules so that citizens will know that they are being asked for only the information that is necessary for the purpose clearly identified on the

³ See discussion, Victoria, Website Privacy—Guidelines for the Victorian Public Sector.

⁴ Cookies are small bits of data that are placed on the user's hard drive. They can enhance the user's experience of a web site by allowing the web site to recognise the user, provide access to specific resources or provide customised web pages. Some cookies, however, raise privacy and security issues since they can be used to track the browsing habits of users or used to gain access to computer resources. Session cookies expire after the user exits the web site and are not considered to be a privacy concern; persistent cookies remain on the user's hard drive and if used for a TTGOV web site, should not contain any personal information. A web beacon (or web bug or pixel tag) is placed on a web site to monitor the behaviour of the user of the site and can give information, including the IP address, the time and for how long the site was viewed, and the type of browser. For information on protecting privacy on the Internet, see, for example, www.privacy.gov.au/internet/internetprivacy
<http://www.ipc.on.ca/docs/primer-e.pdf>

web site, that the information will be used for only that purpose, and that the information will be secure from unauthorized disclosure. They will know that they can reach a named official if they have questions or if they want to challenge or change the personal information being held by government. In short, citizens will be able to place their trust in government with respect to the confidentiality of their personal information.

9. Policy Prescriptions

9.1 Requirements of TTGOV web sites include:

9.1.1 General Obligations for Protection of Personal Privacy

Policy Guideline: **Required**

Each Ministry, department and agency must comply with the Data Protection Policy approved by Cabinet in January 2006.

9.1.2 Privacy Impact Assessments

Policy Guideline: **Required**

Each Ministry, department and agency must perform a Privacy Impact Assessment of the activities and information to be placed on or collected by any web site for which it is responsible.

Policy Guideline: **Required**

Each Ministry, department and agency must renew the Privacy Impact Assessment whenever a web site or government program being delivered via a TTGOV web site is significantly re-designed.

9.1.3 Privacy Statements

Policy Guideline: **Required**

Every TTGOV web page must link to a privacy statement that clearly states what personal information is being collected and the use that will be made of the information.

Policy Guideline: **Required**

Each Ministry, department and agency must inform the user of the implications of not providing some or all of the information on the web site.

Policy Guideline: **Required**

Each Ministry, department and agency must not use “persistent” cookies or web beacons on its web site.

9.1.4. Security of Personal Information

Policy Guideline: **Required**

Each Ministry, department and agency must ensure that personal data that is collected by or through a TTGOV web site is secure.

Policy Guideline: **Required**

Each Ministry, department and agency must ensure that access rights to personal information are provided only to those officials who actually require access for the purposes that were stated at the time of collection or for consistent purposes.

9.2 Recommended standards for TTGOV web sites include:

9.2.1 General Obligations for Protection of Personal Privacy

Policy Guideline:

Recommended

Each Ministry, department and agency must assign and document responsibilities for protection of personal data collected through TTGOV web sites.

Policy Guideline:

Recommended

Each Ministry, department and agency should ensure that its staff is adequately trained in the requirements of the Data Protection Policy and are aware of and sensitive to the need to protect personal privacy.

9.2.2 Privacy Impact Assessments

Policy Guideline:

Recommended

Each Ministry, department and agency should carefully consider and identify what personal information is required to carry out its activities to ensure that no unnecessary personal information is collected.

Policy Guideline:

Recommended

Each Ministry, department and agency should consider the use of privacy enhancing technologies (PETs) and system design techniques when developing TTGOV web sites that will collect personal information.

9.2.3 Privacy Statements

Policy Guideline:

Recommended

Each Ministry, department and agency should consider using multi-layered formats for privacy statements, with a short statement containing the minimum required information that is linked to a longer and more complex statement.

Policy Guideline:

Recommended

Each Ministry, department and agency should conduct user testing to ensure that readers of a simplified privacy notice find it user-friendly and comprehensible.

Policy Guideline:

Recommended

Each Ministry, department and agency should include information about such technologies as session cookies in its more comprehensive privacy statement.

9.2.4. Security of Personal Information

Policy Guideline:

Recommended

Each Ministry, department and agency should document the security procedures for the collection, transmission, storage and disposal of personal information and the access to that information.

Policy Guideline:

Recommended

Each Ministry, department and agency should ensure that authorization controls are in place to clearly identify which officials are authorised to add, change or delete personal information from records.

Policy Guideline

Recommended

Each Ministry, department and agency should ensure that procedures and systems are in place so that access and changes to personal information can be audited by date and user identification.

Policy Guideline

Recommended

Each Ministry, department and agency should ensure that procedures and systems are in place to identify security breaches or erroneous disclosures of personal information in error and that contingency plans are developed to notify appropriate parties of such breaches or disclosures.

10. References

1. Australia, Office of the Privacy Commissioner, Managing Privacy Risk, An Introductory Guide to Privacy Impact Assessment for Australian Government and ACT Government Agencies, Consultation Draft, November 2004.
2. Australia, Victoria, Victorian Privacy Commissioner, Website Privacy—Guidelines for the Victorian Public Sector, May 2004.
<http://www.privacy.vic.gov.au/dir100/priweb.nsf/content/960AFEC70211142FCA256FB900102E91?OpenDocument>
3. Australia, Victoria, Victorian Privacy Commissioner, Privacy Impact Assessments—A guide, August 2004.
<http://www.privacy.vic.gov.au/dir100/priweb.nsf/content/960AFEC70211142FCA256FB900102E91?OpenDocument>
4. Canada, Alberta, Office of the Information and Privacy Commissioner, Privacy Impact Assessment: Instructions and Annotated Questionnaire, January 2001;
5. Canada, British Columbia, Ministry of Labour and Citizen's Services, Privacy Impact Assessment Process.
6. Canada, Manitoba, Ombudsman, Privacy Compliance Tool: Checklist at a Glance, October 2003.
7. Canada, Treasury Board Secretariat, Privacy Impact Assessment Policy.
8. Karol, Thomas J., Cross-Border Privacy Impact Assessments: An Introduction, Vol.3, 2001 Information Systems Control Journal.
9. Ireland, Data Protection Commissioner, Assess your own Data Protection Policy. <http://www.dataprivacy.ie/viewdoc.asp?DocID=22>
10. Ireland, Data Protection Commissioner, Guidelines for the contents and use of Privacy Statements on Websites.
<http://www.dataprivacy.ie/viewdoc.asp?m=m&fn=/documents/guidance/PrivStatements.htm>
11. New Zealand, Office of the Privacy Commissioner, Privacy Impact Assessment Handbook, <http://www.privacy.org.nz/library/privacy-impact-assessment-handbook>
12. New Zealand, State Services Commissioner, ICT Division, Privacy Impact Assessment of the Proposed Government Logon Service, 2005.
<http://www.e.govt.nz/services/authentication/gls-pia/>
13. Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, Making Privacy Notices Simple, 24 July 2006.
14. United States, Office of Management and Budget, Guidance and Model Language for Web Site Privacy Policies, June 1, 1999.
<http://www.whitehouse.gov/omb/memoranda/m99-18attach.html>
15. United States, Office of Management and Budget, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.
<http://www.whitehouse.gov/omb/memoranda/m03-22.html>

Sample Privacy Impact Assessment Checklist

Privacy Principle 1: Accountability for Personal Information

1. Has responsibility for the PIA been assigned?
2. Is there a privacy coordinator or other “champion” in the ministry, department or agency?
3. If third parties (e.g., a private sector entity or individual or another government ministry, department or agency) are involved in the custody or control of the information, have agreements been put in place that establish privacy requirements and safeguards?
4. Does a documented management reporting process exist to ensure that management is informed of any privacy compliance issues?
5. Is senior management actively involved in the development, implementation and promotion of privacy measures within the organization?

Privacy Principle 2: Collection and Identifying Purposes

6. Is there a detailed description of the personal information or personal data elements that are being collected for this program or initiative? (personal information includes such information as an individual's name, address or telephone number, race, ethnic origin, religious beliefs or associations, age, sex, sexual orientation, marital or family status, or any identifying number or symbol assigned to the individual)?
7. Is all the personal information being collected necessary for the operating program or activity?
8. Are there any requirements in the legislation that authorizes the program or policy that affect the management of personal information?
9. Is there authority (e.g., legislation or order) for the collection of the personal information?
10. Is there notice at the collection stage that identifies the purposes for the collection, the authority for the collection and an official contact person?
11. Are secondary uses for the personal information being contemplated?
12. If personal information is being used or disclosed for a secondary purpose not previously disclosed or identified, is consent required?
13. Is information anonymized when used for planning, forecasting, evaluation or other analytical purposes?

14. Is the personal information being collected directly from the individual? If not, why not?

Privacy Principle 3: Consent

15. Is consent obtained directly from the individual? If not, why not?
16. How is consent obtained?
17. Does consent require a positive action (e.g., clicking on an icon) by the individual?
18. Is the consent clear and unambiguous?
19. Can the individual refuse to consent to the collection or use of personal information for a secondary purpose, unless required by law?
20. Will the refusal of an individual to consent to the collection or use of personal information for a secondary purpose have an effect on the level of program service provided to the individual?
21. Are there any standards or mechanisms in place to ensure that the individual has the capacity to give consent?
22. Are there standards and mechanisms in place to allow for another authorized person to give consent for an individual who does not have the capacity for consent (e.g., a minor)?

Privacy Principle 4: Use of Personal Information

23. What is the legal authority to use personal information?
24. Is the personal information to be used exclusively for the purpose for which it was originally obtained?
25. Are the uses of the information limited to what a reasonable person would consider appropriate in the circumstances?
26. Is the information being used for a purpose that is consistent with the original purpose for which it was collected?
27. Is the personal information being used for a purpose that requires the disclosure of the information to another government institution?
28. Is there data matching, either between data bases within a ministry, department or agency or between ministries, etc.?

Privacy Principle 5: Disclosure and Disposition of Personal Information

29. Is personal information being disclosed with the consent of the individual?

- 30. If personal information is not being disclosed with consent, has specific authority for disclosure been identified?
- 31. Will the personal information to be disclosed be limited to the purposes of disclosure?
- 32. Will personal information be collected, processed, used, retained or disclosed outside of Trinidad and Tobago?
- 33. Is the personal information scheduled for disposal?⁵
- 34. If so, what procedures are being used for disposal?

Privacy Principle 6: Accuracy of Personal Information

- 35. What steps will be taken to ensure that the personal information is accurate, up-to-date and complete?
- 36. Does the record of personal information indicate when the information was last updated?
- 37. Is a record kept of the source of the information used to make changes?
- 38. Is there a procedure to provide notice of correction to third parties to whom the information has previously been disclosed?
- 39. Is a record kept of requests for reviews of errors or omissions?
- 40. Is there a clearly defined process by which an individual may access and dispute the accuracy of the personal information?

Privacy Principle 7: Security and Safeguarding Personal Information

- 41. Has the risk assessment associated with the web site dealt with issues of the protection of personal privacy?⁶
- 42. Have arrangements been made for the secure custody or control of the information?
- 43. Do privacy controls deal with such measures as “need to know” policies and procedures for access to personal information?
- 44. Are security measures commensurate with the sensitivity of the information?
- 45. Are program and information technology staff trained in the requirements for protecting personal information?
- 46. Has a plan been prepared that indicates the flow of information and identifies the persons, positions or employee categories that will have access to personal information?
- 47. Will personal information be disclosed to any persons who are not TTGOV employees?

⁵ See also, Policy on Electronic Records (draft).

⁶ See also, Policy on Risk Management (draft).

48. If personal information will be used in the electronic delivery of services, have technological tools and system design techniques been considered that may enhance privacy and security (e.g., encryption, anonymity or pseudo-anonymity procedures)?
49. Is there a documented process in place to authorize any modification (e.g., addition, deletion, correction) of personal information?
50. Is there a documented process in place to respond to security breaches or disclosures of personal information in error?
51. Is there a documented process in place to communicate security breaches to the data subject and relevant authorities (e.g., program managers, law enforcement authorities)?
52. Can the process to modify personal information be audited (e.g., date and identify of person making changes)?

Privacy Principle 8: Openness

53. Is there a communication plan to explain to the public how their personal information will be handled (e.g., managed, shared, protected)?
54. Have key stakeholders had an opportunity to comment on the privacy protection implications of the activity or program?
55. Is there a Privacy Notice on the web site?

Privacy Principle 9: Individual's Access to Personal Information

56. Is there a documented process in place to ensure that an individual can have access to his or her personal information?
57. Is there a documented process in place to ensure that an individual is notified if a correction is made to his or her information?
58. Are all those with custody or access to personal information aware of an individual's right of access and the process in place to handle complaints, modifications, etc.?

Privacy Principle 10: Challenging Compliance

59. Is the complaint process for the program or service consistent with the Data Protection Policy?
60. Is there a documented process to regularly review the nature, frequency and resolution of complaints in order to improve information management practices?

61. Have arrangements been made to review or audit compliance with procedures, techniques and systems to protect personal privacy and general compliance with the Data Protection Policy?