

Tasmanian Government Information Security Framework

Tasmanian Government Information Security Charter

Version 1.0 – May 2003

1 Purpose

The Tasmanian Government is responsible for the information assets it holds in order to carry out its functions. These assets must be safeguarded from sources of harm that would compromise or destroy them. Types of threats include criminal, political, natural, and accidental; types of harm include loss, damage, corruption, and disclosure.

While the Government as a whole is responsible for the security of its information assets, individual Ministers are responsible for the operation of their portfolios. In practice, the day-to-day management of information security arrangements in an agency is the responsibility of the agency head.

Each agency must create and maintain an appropriate security environment for the protection of its information assets. The Government requires each of its agencies to identify those information assets vital to the community and the operation of the Government. Security measures will need to be employed to ensure that these assets are safeguarded.

The purpose of this charter is to provide a whole of government framework to enable the government to manage security risks to its information.

2 Background

Information security measures are usually a combination of physical, personnel, and information and communication technologies (ICT) security measures. These measures are sometimes expensive to implement and might have an impact on agency operations.

In addition, the Government needs to be assured that **information security measures are only used when the risk warrants it and the security measures used are appropriate to the identified risk.**

Agencies that do not provide an appropriate security environment for their information assets place at risk the Government at large, not just themselves. The compromise of government information assets will also damage both the public interest and the public's confidence in the Government.

Many of the principles outlined below have implications for general security policies, not just information security policies.

3 Context

In an ideal world an information security framework exists within the context of a whole of government general security policy.

Accordingly the whole of government information security policy has been developed with the assumption that there is a whole of government general security policy which contains, at a minimum, the following principles:

- (a) An effective security environment is essential for an agency to function efficiently and effectively.

- (b) Each agency head is responsible to their Minister for ensuring that the functions performed, the assets held, the people employed and the clients serviced by the agency are protected against unacceptable risk.

4 Legislative Requirements

The Tasmanian Government Information Security Charter has been endorsed by Government as policy for Government Agencies (in defined in, Schedule 1, Part 1 of the *State Service Act 2000*).

There are a number of statutes that impose security and information security requirements on all agencies, these include:

- The State Service Principles of the *State Service Act* require the State Service to be accountable for its actions and performance [s7(1)(d)]. Heads of Agencies must uphold, promote and comply with the State Service Principles [s8].
- All employees (including heads of agencies and officers) must comply with the State Service Code of Conduct. Under the Code of Conduct an employee must maintain appropriate confidentiality about dealings of, and information acquired by, the employee in the course of that employee's State Service employment [s9(7)].
- Agencies are to preserve all records until dealt with as provided by the *Archives Act 1983* [s10(1)].
- General security - *Financial Management and Audit Act 1990* makes the Head of Agency responsible for the custody, control, management of and accounting for, all public property, public money, other property and other money in the possession of, or under the control of, that Agency [s22(e)].

In addition other statutes impose information security requirements on specific agencies and/or business units of agencies.

5 Information Security Policy Principles

The principles underlying the Information Security Policies are as follows:

1. Each agency must develop and implement an Agency Information Security Plan that is appropriate to the agency's functions and the risks that it faces.
2. The Agency Information Security Plan needs to identify the information assets of the agency.
3. Each agency is to conduct regular information security risk assessments.
4. The Agency Information Security Plan needs to be monitored and reviewed to minimise information security risks.
5. Information resources, including ICT systems, to be reasonably protected from compromise and misuse – that is, the range of means by which harm could be caused to information, especially loss, damage, corruption, or disclosure, whether deliberate or accidental.

6. People employed to perform Government functions to be suitable and meet relevant standards of integrity and honesty.¹
7. When outsourcing a function, agencies remain accountable for the secure performance of that function.
8. Information resources used in a home-based or mobile environment are suitably secured.

6 Information Security Policies

1. Governance

Agencies are to manage information security through the establishment of a management framework to initiate and control the implementation of information security within the agency.

2. Record Security

Agencies are to implement appropriate record security policies and procedures as part of their records management policies and procedures to ensure the security of information access, transmission, storage and destruction.

3. Physical Security for Information Security

Agencies are to ensure appropriate physical security measures are adopted to prevent unauthorised access, damage, loss or interference to agency information, information systems, services or equipment.

4. Personnel

Agencies are to actively inform personnel who have access to agency information resources of their roles and responsibilities in regard to information security.

Personnel is defined to include officers, employees², contractors, and students.

5. General IT

Agencies are to have a comprehensive framework governing all aspects of information and communication technologies security.

6. Incident Reporting

Agencies are to minimise the damage from information security incidents and monitor and learn from such incidents.

¹ In accordance with the *State Service Act 2000* (Code of Conduct s.9).

² Officers and employees as defined in the *State Service Act*.

7 Primary Responsibilities and Roles in Information Security

7.1 Drafting & Maintaining the Information Security Policies and Guidelines

The Secretary of the Department of Premier and Cabinet, in consultation with agencies, is to draft and maintain the:

- Tasmanian Government Information Security Charter, which includes information security policy principles and information security policies; and
- Tasmania Government Information Security Framework, which includes guidelines to assist in implementing the Charter.

7.2 Implementation of Information Security Policies and Guidelines

Heads of Agencies are to implement the Tasmanian Government Information Security Charter using the Tasmanian Government Information Security Framework as a guide.



Tasmania
Explore the possibilities

Inter Agency Policy and Projects Unit
Department of Premier and Cabinet

Post: GPO Box 123
Hobart TAS 7001
Ph: 6233 3836
Email: iappu_enquiries@dpac.tas.gov.au
Visit: www.egovernment.tas.gov.au

Published May 2003
ISBN 978 0 7246 5591 3
© State of Tasmania