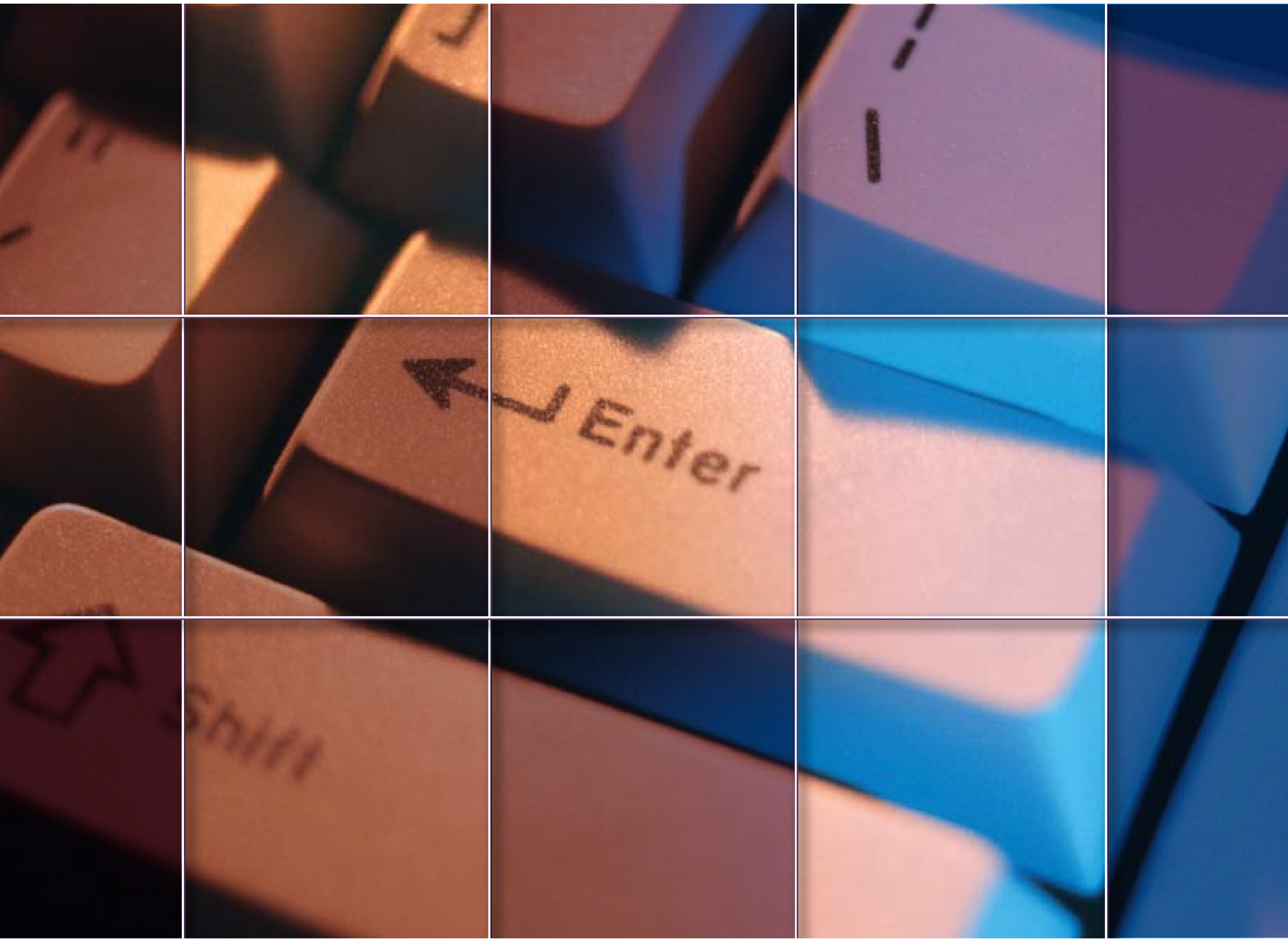
STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga

Trusted Computing and Digital Rights Management Principles & Policies



DEVELOPMENT GOALS

e-government
www.e.govt.nz

State Services Commission
September 2006
Version 1.0
ISBN 978-0-478-30301-8

Trusted Computing and Digital Rights Management Principles & Policies

Preface to Principles and Policies

Introduction

The New Zealand Government Trusted Computing and Digital Rights Management Principles and Policies were developed in 2006 in anticipation of the growing usage of trusted computing and digital rights management technologies. The aim of the principles and policies is to ensure that the use of trusted computing and digital rights management technologies does not adversely affect the integrity (including availability and confidentiality) of government-held information or related government systems.

The Principles and the Policies have been drafted with the intention of universal applicability – to be relevant in overseas jurisdictions as well as in New Zealand. Therefore, requirements or references peculiar to New Zealand (for example, references to New Zealand's Privacy Act) are omitted from policy statements, and are confined to the 'Scope and Interpretation' sections that accompany each statement.

Trusted computing and digital rights management are emerging technologies, and their use and development are only beginning to be realised. Their characteristics and functionalities, and the ways that they can be used, are expected to evolve and change significantly over time.

These technologies promise some advancement for the security and management of information, and many expect their use to become ubiquitous - potentially incorporated within every conceivable type of electronic device.

At the same time, these technologies present challenges and risks to government in the protection of the integrity of government-held information. In response to such challenges, and to mitigate the risks, the New Zealand government has developed this set of principles and policies for the use of these trusted computing and digital rights management technologies.

Trusted Computing and Digital Rights Management - Uncertainty of Definition

The definitions for the terms "trusted computing" and "digital rights management" are still being widely debated. Some definitions focus on specifications for the software and hardware. Some focus on their **functionality** and what they will do. Others focus on who will have **control** of the functionalities.

Basic definitions for each of these terms have been included within the glossary to this paper, to provide some helpful context for the principles and policies. But it is acknowledged that these are indicative only.

Integrity of Government-held Information - Certainty of Definition

The underlying tenet for the development of these principles and policies has been the protection of the integrity of government-held information. While the implications of trusted computing and digital rights management have been the catalyst for this work, the focus has been on the obligations and responsibilities of government.

This has enabled certainty in our work in the context of the uncertainty of these emerging technologies. Our aim has been to develop principles and policies that will remain valid regardless of how the technologies may evolve and be implemented.

"TC/DRM" Used Instead for the Purposes of this Paper

The term "TC/DRM" has been used in this paper to refer to trusted computing and/or digital rights management, functioning separately or working together. This does not mean that the terms are considered to be interchangeable: it is acknowledged that trusted computing and digital rights management are distinctly different technologies. However, they each offer some similar risks to the integrity of government held information, and will have the potential to mutually reinforce each other. "TC/DRM" is a convenient term to represent any of a wide range of potential manifestations of the technologies.

The principles and policies reflect the importance to government of its being able to continue to exercise control of its data and computing environments, in order to ensure the integrity of its information. TC/DRM technologies have the potential to enhance or diminish that control, depending on how they may be deployed. The extent to which it may be appropriate for government to make use of these technologies will be a function of the degree of control it is able to continue to exercise, and the consequent risks to the integrity of information it holds. These principles and policies have been developed to support this risk assessment and decision-making process.

The principles and policies will establish a framework within which individual agencies can develop operational practices, appropriate for their own business drivers and statutory responsibilities. Some guidance will be provided through the development of practice notes to assist agencies with this important work.

Framework for Principles, Policies & Standards

Principles…

are fundamental truths, laws or requirements as the *basis* for reasoning or action.

Principles have the following characteristics:

- they articulate the basis - the *"Why"* - of the Policies;
- they reflect concerns, risks, issues, and emphases;
- adherence to them is *qualitatively assessable*.

Policies…

are high-level courses of action.

Each policy statement is accompanied by a scope and interpretation section, and a rationale. Each policy supports one or more of the principles.

Policies have the following characteristics:

- they deal with *"What"* we will do to implement the Principles;
- adherence to them is *qualitatively assessable*.

Standards…

generally set out specific, measurable or observable goals that support the policies.

The goals may be behavioural, though they may be implemented by means of systems.

Standards have the following characteristics:

- deal with *"How"* we will implement the Policies;
- adherence to them is *measurable or observable*.

PRINCIPLES

Principles for government use of Trusted Computing and Digital Rights Management technologies

INFORMATION AVAILABILITY PRINCIPLE

1. For as long as it has any business or statutory requirements to do so, government must be able to:

- use the information it owns/holds;
- provide access to its information to others, when they are entitled to access it.

INFORMATION CONFIDENTIALITY AND INTEGRITY PRINCIPLES

2. Government use of trusted computing and digital rights management technologies must not compromise the privacy rights accorded to individuals who use government systems, or about whom the government holds information.

3. The use of trusted computing and digital rights management technologies must not endanger the integrity of government-held information, or the privacy of personal information, by permitting information to enter or leave government systems, or be amended while within them, without prior government awareness and explicit consent.

SYSTEM SECURITY PRINCIPLE

4. The security of government systems and information must not be undermined by use of trusted computing and digital rights management technologies.

Summary of Principles and Policies

Information Availability Principle

For as long as it has any business or statutory requirements to do so, government must be able to:

- **use the information it owns/holds;**
- **provide access to its information to others, when they are entitled to access it**

Information Availability Policies

1. Informed consent to externally-imposed digital encumbrance

Any information that is relied on for execution of public business must be free from encumbrance by externally-imposed digital restrictions, except with the informed consent of government.

2. Conditions for externally-imposed digital encumbrance

If information is required for execution of public business, and is externally encumbered:

- the agency must have full knowledge of the rights when consenting to the encumbrance;
- the agency must be notified that an encumbrance exists, and be able to easily view the rights, at each use;
- the rights must be fixed, except by mutual consent of the agency and the rights-holder
- the rights assigned must be adequate for the uses of the information, including use by officials with responsibilities to audit and review.

3. Control of digital encumbrances

Any DRM encumbrance applied to the government's master copy of any information it owns, must be under the government's full and exclusive control.

4. Usage by all legitimate parties

When implementing solutions involving TC/DRM, agencies will ensure that adequate provision is made for the use of any information, at present and in the future, by all parties with statutory rights to use that information.

5. Assurance of future accessibility

If agencies' use of hardware or software can be limited by TC/DRM technologies, and access to information is reliant on that hardware or software, then agencies will take appropriate measures to ensure future accessibility of that information.

6. Minimum constraint on usage

Agencies will apply digital encumbrances to information only if there is a clearly identified business reason for doing so, and will apply only the minimum necessary degree of constraint.

7. Common privilege definitions

Agencies protecting information with TC/DRM encumbrances will use a common set of digital rights definitions, to ensure that access requirements are met consistently.

8. Independent usage capability

Agencies will apply TC/DRM restrictions to information only if a means to take full control of the access rights is vested in a designated independent government agency.

9. Modification/deletion by hardware/software

Agencies must not operate hardware or software with functionality that could modify, or hinder access to, information held by government, without explicit government approval.

Information Confidentiality and Integrity Principles

Government use of trusted computing and digital rights management technologies must not compromise the privacy rights accorded to individuals who use government systems, or about whom the government holds information.

The use of trusted computing and digital rights management technologies must not endanger the integrity of government-held information, or the privacy of personal information, by permitting information to enter or leave government systems, or be amended while within them, without prior government awareness and explicit consent.

Information Confidentiality and Integrity Policies

10. Awareness of TC/DRM functionality

When deploying hardware or software, or using information provided by an external party, agencies will take all reasonable measures to ensure that they are aware of the inclusion of TC/DRM functionality.

11. Knowledge of information flows

Agencies must know enough about any information flows into or out from their TC/DRM systems that could involve collection or transmission of personal information, to ensure knowledge and acceptance of:

- when such events occur;
- what is collected or transmitted;
- the purpose of collection;
- who is collecting the information;
- who will receive and/or share the information;
- for how long they will hold the information, and under what conditions; and
- if applicable, who will amend and update the information and how it will get done.

12. Communications specifications

Agencies will operate a TC/DRM solution only if:

- a specification is provided that documents the triggers and content of any communications (including attestation and other background communications) that leave from or arrive at the computer, and
- the solution does not perform any communications that are not described in the communications specification, and
- any communications that would be unacceptable to government can be 'opted out of'.

The solution should be verified for conformity to the communications specification by a competent authority recognised by the government for this purpose.

System Security Principle

The security of government systems and information must not be undermined by use of trusted computing and digital rights management technologies.

System Security Policy

13. Ability to identify harmful communications

Agencies will reject the use of TC/DRM mechanisms, and information encumbered with externally imposed digital restrictions, unless they are able to satisfy themselves that the communications and information are free of harmful content, such as worms and viruses.

Interpretation of the Principles and Policies

Information Availability Principle

For as long as it has any business or statutory requirements to do so, government must be able to:

- use the information it owns/holds;
- provide access to its information to others, when they are entitled to access it

1. Informed consent to externally-imposed digital encumbrance

Any information that is relied on for execution of public business must be free from encumbrance by externally-imposed digital restrictions, except with the informed consent of government.

Rationale

Restrictions on the usage of information may hinder an agency's ability to do business and keep adequate records. Agencies need to know when an encumbrance exists, so that they can either refuse to accept the information on those terms, or can take appropriate measures to manage the risk.

This policy ensures that agencies that accept information with usage restrictions, do so with prior knowledge and hence with the opportunity to satisfy themselves that there is no negative impact, or that adequate mitigations are available.

Supports Information Availability principle.

Scope & Interpretation

This policy will generally be relevant in situations where information is to be held but not 'owned' by government, and thus there may be a legitimate reason for the information to be externally encumbered. By contrast, Policy 3, 'Control of digital encumbrances', will apply in situations where the information is owned by the government, and therefore there is no legitimate reason for an external party to control the digital rights.

Agencies should generally be attempting to have information unencumbered to support the process of government, or at the very least to have it able to be copied to an unencumbered public record. Simply identifying that a legitimate (which can be commercial) reason exists for the encumbrance is not in itself justification to allow encumbered data into government.

Refer to Glossary: DRM, for types of encumbrance likely to be encountered under TC/DRM.

"free from encumbrance by externally-imposed digital restrictions" refers to freedom from digital restrictions on usage imposed from outside the New Zealand government.

The notion of "informed consent" has two parts:

- "informed" requiring adequate advice to government and sufficient understanding by government to appreciate the implications for the integrity of government-held information (Policy 2 helps elaborate on how this might be achieved), and
- "consent" requiring active decision-making in each case.

"informed consent of government" will therefore apply when a person in an agency, authorised to make such a decision on an agency's behalf, is aware of the encumbrance (or the possibility of it) and with that awareness and an understanding of the implications, accepts the information. It is possible that the detection and consent process could be delegated to rules-based software, which could either:

- acknowledge the possibility of an encumbrance, but determine the information to be of a category for which an encumbrance does not matter, or
- positively detect an encumbrance, identify the nature of the encumbrance and the category of information it is applied to, and accept it on the basis of consent criteria being satisfied.

Informed consent could potentially be achieved by development of a specific trust relationship between recipient and provider, if a provider were to make a general undertaking either to not use DRM, or to use it only within specific boundaries.

The basis/rationale for the "consent" decision needs to be recorded.

Categories of information for which external encumbrance may not compromise the public record

The Public Records Act 2005 sets up a very broad definition of "public record". Within that definition, the Chief Archivist has authorised several classes of routine or trivial records for destruction as soon as they are no longer administratively required. These will be described in a future Trusted Computing and Digital Rights Management Standards and Guidelines document.

For these classes of material, it is possible that encumbrance may be allowed without compromising the public record. However, if such routine information is subsequently used in official business (e.g. information sourced from a discussion list is used as a basis for formal action) an adequate record should be captured without encumbrance.

Categories of information that should rarely, if ever, be subject to external encumbrance

Information that should rarely, if ever, be subject to external encumbrance, is that which is relied upon in the course of public business (e.g. for decision-making, policy setting), or which provides the basis for citizen rights. In such cases, agencies should create an adequate, unencumbered record of relevant information.

2. Conditions for externally-imposed digital encumbrance

If information is required for execution of public business, and is externally encumbered:

- **the agency must have full knowledge of the rights when consenting to the encumbrance;**
- **the agency must be notified that an encumbrance exists, and be able to easily view the rights, at each use;**
- **the rights must be fixed, except by mutual consent of the agency and the rights-holder;**
- **the rights assigned must be adequate for the uses of the information, including use by officials with responsibilities to audit and review.**

Rationale

This policy ensures that the information continues to be fit for purpose. Each user will be sufficiently informed of any usage restrictions, such that if a mitigating action (e.g. making a file note) is required on their part to maintain fitness for purpose, they will be aware of it.

Supports Information Availability principle.

Scope & Interpretation

Refer to Glossary: Rights for a definition of this term.

Notification of an encumbrance will enable users to know whether they need to record separate notes.

Encumbered information may be used multiple times by multiple officials. On each use, they need to know:

- whether the information is encumbered;
- what the details of the encumbrance are.

This will require some form of alert to users in an agency on each usage of the information so that they are aware that an encumbrance exists, and a means for finding out what the encumbrance is.

“rights must be fixed” means that the digital rights with which the information is encumbered, must not be subject to alteration or revocation.

Example: The subsequent addition of an access expiry date, or the revocation of a user’s ability to perform a particular function on the information, such as printing it.

The clause allowing rights to be changed “by mutual consent of the agency and the rights-holder”, is intended primarily to allow for subsequent relaxation of the rights, in order to accommodate the needs of the agency. Agencies should exercise care in agreeing to any other sort of change because the usage needs may be well understood at the time the information is first received and used, but after the fact may not be well known or in fact forgotten. In situations when a request is made to vary the terms of restriction, it may not be possible for the agency representative to know what use had been made of the information in the past. If the consent activity is not “fully informed”, it must not proceed.

3. Control of digital encumbrances

Any DRM encumbrance applied to the government's master copy of any information it owns, must be under the government's full and exclusive control.

Rationale

This policy ensures that government will not lose the ability to maintain control over its intellectual property, and the use of its information.

Supports Information Availability principle.

Scope & Interpretation

As well as applying this policy in a technical context, government agencies will need to apply it when negotiating contracts for project and development work that is expected to result in production of information which the government will own. Stating in the contract that such information must either be unencumbered, or that the encumbrance must be under the government's control, will:

- reduce the likelihood of subsequent disputes with vendors;
- reduce the likelihood of DRM encumbrances being inadvertently applied by the vendor.

'Master copy' refers to the copy of the information regarded as authoritative and identified as such, and from which other copies may be made. A master copy may consist of multiple versions, as each of these may have significance for record-keeping or administrative purposes. Backups of the master copy are considered part of the master copy. Copies made for other purposes are not.

This policy will apply in situations where the information is *owned* by the government, and therefore there can be no legitimate reason for an external party to control the digital rights. By contrast, Policy 1, 'Informed consent to externally-imposed digital encumbrance', will generally be relevant in situations where information is to be held but not 'owned' by government, and thus there may be a justified reason for an agency to accept the information with an external encumbrance.

4. Usage by all legitimate parties

When implementing solutions involving TC/DRM, agencies will ensure that adequate provision is made for the use of any information, at present and in the future, by all parties with statutory rights to use that information.

Rationale

This policy ensures that agencies consider the full range of information usage requirements when implementing TC/DRM solutions.

Supports Information Availability principle.

Scope & Interpretation

Statutory rights to hold and use information derive from the Public Records Act, Privacy Act, Official Information Act and other legislation.

Relevant parties with statutory rights may include individuals, Archives New Zealand, and other agencies.

TC/DRM technologies can be used to restrict usage of information. It is expected that there will be much less flexibility to reverse, suspend or bypass these restrictions, than with conventional technologies currently in use by government agencies. Therefore, if TC/DRM restrictions are applied to information and some present or future access requirement is not provided for, there will be less chance of finding a way to satisfy the requirement, compared with if conventional technologies had been used.

Inadequate provision for legitimate access may take the following forms:

- the need for access was overlooked by the agency applying the restrictions, or
- the need for access was recognised, but the agency applying the restrictions made insufficient provision to ensure that the management and technical prerequisites for access were, and would continue to be, satisfied.

Agencies need to ensure that provision for use is made:

- for information stored within their own organisation
- for information they have sent to other parties with statutory rights to use that information.

Agencies making use of TC/DRM for communications, must do so only if all intended recipients have reasonable access to the technology required to permit use of the information.

Example: If a DRM-protected document is sent to a recipient and that recipient requires internet access for authentication, the recipient must either have internet access, or the document must be made available to them in an alternate, usable form.

When considering what ‘future’ encompasses, agencies should consider issues such as usage expiry mechanisms, provision for data migration, etc.

5. Assurance of future accessibility

If agencies' use of hardware or software can be limited by TC/DRM technologies, and access to information is reliant on that hardware or software, then agencies will take appropriate measures to ensure future accessibility of that information.

Rationale

This policy ensures that future access to information is not inadvertently lost as a result of TC/DRM restrictions on the use of the hardware or software normally used to access the information.

Supports Information Availability principle.

Scope & Interpretation

Agencies must ensure that the functioning of hardware or software required to maintain government information, cannot be impeded by influences outside government control.

Example: For instance, a software application might contain a start-up test that blocks access to the application's normal functionality if it cannot successfully perform an online validation check with the software vendor's network. Such 'heartbeat' functionality could cause agencies to be hindered from accessing or processing their data through circumstances outside of their control, so would not be acceptable unless there was a suitable bypass mechanism or process available to them.

Alternatively, agencies must adopt mitigation strategies to ensure continued access to information if government's use of the software or hardware were to be externally constrained.

If access to government information is reliant on an agency's hardware or software, and the operation of the hardware or software relies on communication with systems outside the control of government, then the agency is not in a position to ensure future accessibility. Therefore, software or hardware relied on for access to government information must be able to operate without reliance on communication with systems outside the control of government.

This policy does not rule out the use of subscription-based software licences or ASP (Application Software Provider) services, but does require that information is readily accessible by some other means should the subscription end.

This policy requires consideration of issues around *future* requirements for migration (both of the information and its associated audit trail) to different platforms, data formats or software products, when implementing TC/DRM *now*. For example, will information created in one environment using particular software be accessible in the future if it needs to be migrated to a different platform or if it has to be accessed using different software? Although these issues are not peculiar to TC/DRM, in some cases the use of TC/DRM will significantly reduce the mitigation options.

6. Minimum constraint on usage

Agencies will apply digital encumbrances to information only if there is a clearly identified business reason for doing so, and will apply only the minimum necessary degree of constraint.

Rationale

Placing usage restrictions on any information inevitably makes it more expensive to manage. The expense is not necessarily confined to the agency, but may also impact other agencies with which the information is shared, or which may subsequently become its custodian (such as Archives New Zealand). In addition, usage restrictions raise the risk that a legitimate user may not have the access to which they are entitled.

Supports Information Availability principle.

Scope & Interpretation

This policy deals with situations where government is creating or changing information, and therefore can choose whether to encumber the information with digital restrictions, and to what extent. In these situations, government is the *originator* of the encumbrance. There are other policies in this framework that address the issues arising when government is instead the *recipient* of encumbered information.

Digital encumbrances may vary along several dimensions – who can access the information, what functions they can perform upon it (e.g. view, print), and how long the rights or restrictions last for. Applying the ‘minimum necessary degree of constraint’ means imposing the least amount of restriction along each of these dimensions.

When considering the ‘minimum necessary degree of constraint’, agencies should include the dimension of time. The need for restrictions may be for a limited time only, in which case the restrictions could be set to expire after a certain date, or could be removed after that date.

7. Common privilege definitions

Agencies protecting information with TC/DRM encumbrances will use a common set of digital rights definitions, to ensure that access requirements are met consistently.

Rationale

When agencies wish to apply TC/DRM encumbrances to their information, they will need to identify the access requirements of other government agencies for their data, and design access rights definitions that support these requirements. There are requirements that apply to all government agencies, such as:

- future availability to Archives New Zealand
- access by the Office of the Controller and Auditor-General
- meeting the requirements of the Protected Disclosures Act

Without a coordinated approach being taken, the cost of analysing the requirements and designing appropriate definitions will be repeated many times, and the results are likely to be inconsistent. Where the results are inadequate, this may not be discovered until a long time after (e.g. hand-over of archival material to Archives New Zealand), and correction could be very expensive at that point.

By taking a coordinated approach, government can develop a uniform, best-practice approach to support generic inter-agency information usage requirements.

Supports Information Availability principle.

Scope & Interpretation

There may be circumstances where government agencies consider it appropriate to apply TC/DRM encumbrances to information they create or hold. An all-of-government standard will be developed to provide a set of definitions that meets the minimum requirements for sharing of information across government.

Each agency will be able to develop an internal set of definitions to meet needs specific to itself, as long as they are compatible with the all-of-government standard.

8. Independent usage capability

Agencies will apply TC/DRM encumbrances to information only if a means to take full control of the access rights is vested in a designated independent government agency.

Rationale

This policy protects against situations in which information has become locked down to such an extent that:

- digital preservation, e.g. migrating to a different platform or application, is hampered, e.g. the agency has lost its key to the information;
- the legitimate whistle-blower process is thwarted;
- investigations by monitoring or investigative agencies (Police, Serious Fraud Office, Audit New Zealand etc) are thwarted;
- on-going use by the agency itself is compromised.

Supports Information Availability principle.

Scope & Interpretation

To ensure a consistent, all-of-government approach, a suitable agency will be assigned this role.

The ability for the designated agency to take full control must not be revocable by any other agency or person, including the originating agency (except by a carefully controlled and documented process with fail safe checking).

Full control means the ability to re-assign the rights, or to remove restrictions altogether, so that any functions that could be performed on the information in unrestricted form are then possible. These might include, for example, the abilities to:

- modify the information and save it with the modifications;
- save the information to a different format.

Full control of the access rights, rather than allowing read access only, is required to enable any necessary transformations required for digital preservation, e.g. migration from an obsolete data format.

It is not envisaged that the designated agency's powers would be used routinely. This policy is intended as a contingency plan to counter the risk of an unintended loss of access to government information.

9. Modification/deletion by hardware/software

Agencies must not operate hardware or software with functionality that could modify, or hinder access to, information held by government, without explicit government approval.

Rationale

This policy is intended to protect government information from unauthorised modification or deletion by TC/DRM solutions.

Supports Information Availability principle.

Scope & Interpretation

One of the risks addressed by this policy is the possibility of software being instructed by the provider to delete (or render inaccessible) files considered unacceptable by the provider, such as those that may appear to have been created using an unlicensed product, or that may otherwise appear to breach the terms and conditions for use of the hardware or software.

‘Explicit government approval’ means that any such modification or deletion of information would happen only with approval by a government official with appropriate authority, rather than through action by software not under government control. This approval process could be effected within an agency; the policy is not intended to suggest the establishment of a centralised “government approval” role.

The policy is not intended to address unintended system malfunctions, such as if software was found to have a bug that resulted in the modification or deletion of information. Rather, it is intended to cover circumstances for which such functionality could have been anticipated – and disclosed to the government – because it was included as part of the product’s design.

Information Confidentiality and Integrity Principles

Government use of trusted computing and digital rights management technologies must not compromise the privacy rights accorded to individuals who use government systems, or about whom the government holds information.

The use of trusted computing and digital rights management technologies must not endanger the integrity of government-held information, or the privacy of personal information, by permitting information to enter or leave government systems, or be amended while within them, without prior government awareness and explicit consent

10. Awareness of TC/DRM functionality

When deploying hardware or software, or using information provided by an external party, agencies will take all reasonable measures to ensure that they are aware of the inclusion of TC/DRM functionality.

Rationale

This policy ensures agencies are aware of the inclusion of TC/DRM functionality when they deploy hardware or software, so that they are then in a position to follow the policies that apply in such circumstances.

The policy is designed to guard against situations such as if:

- an agency purchases digital content, which is accompanied by software that enforces digital restrictions, and the software is installed either without the agency's awareness or without the agency realising that it has TC/DRM functionality; or
- an agency installs hardware, which includes TC/DRM functionality to periodically report on the system configuration and its use to some external party, without the agency's knowledge or explicit permission.

In the situations described above, the agency is unaware that it had just installed a TC/DRM solution, and is therefore in no position to comply with the policies that apply when installing a TC/DRM system.

Supports all four TC/DRM principles.

Scope & Interpretation

"Functionality" refers to algorithms capable of performing activity when certain conditions are met, e.g. enforcing digital restrictions, or communicating information about system configuration to external parties. It refers neither to the passive digital restrictions tags that may accompany information, nor to information being received in an encrypted state.

"Reasonable measures" will need to be determined by each agency based on the level of risk in each instance. The level of risk will be directly tied to the nature of the relationship between the deployment and the effect on the integrity of government-held information. Such measures may, for example, include:

- explicit declaration or warranty from the solution provider;
- independent certification by an authority approved by the government.

The reputation of the provider, the contents of the end user licence agreement (EULA), and the presence or absence of Centre for Critical Infrastructure Protection (CCIP) advisories, may be taken into account.

Agencies should note that digital content may be accompanied by auto-installing TC/DRM software, designed to enforce digital restrictions on the content, and possibly on other content as well. Such software may attempt to install without notifying the user, and may attempt to hide its presence and operation once installed. Measures will be necessary to guard against such activity.

11. Knowledge of information flows

Agencies must know enough about any information flows into or out from their TC/DRM systems that could involve collection or transmission of personal information, to ensure knowledge and acceptance of:

- **when such events occur;**
- **what is collected or transmitted;**
- **the purpose of collection;**
- **who is collecting the information;**
- **who will receive and/or share the information;**
- **for how long they will hold the information, and under what conditions; and**
- **if applicable, who will amend and update the information and how it will get done.**

Rationale

Knowledge of the information flows is necessary in order for agencies to be sure that operation of their systems will not lead to contravention of the Privacy Act, either by themselves or by a third party.

Supports Information Confidentiality and Integrity principles.

Scope & Interpretation

Agencies must ensure that users of their systems are informed, as prescribed by the Privacy Act, when information is collected about them.

Agencies must ensure that personal information collected by their systems is protected as prescribed by the Privacy Act, and not kept longer than required for its lawful purpose. This poses a particular challenge if personal information is forwarded to an external party, e.g. as part of a remote attestation process.

If use of TC/DRM technology results in collection or transmission of personal information, then agencies also need to take into account how their obligations and responsibilities under other legislation other than the Privacy Act might be affected.

12. Communications specifications

Agencies will operate a TC/DRM solution only if:

- **a specification is provided that documents the triggers and content of any communications (including attestation and other background communications) that leave from or arrive at the computer, and**
- **the solution does not perform any communications that are not described in the communications specification, and**
- **any communications that would be unacceptable to government can be 'opted out of'.**

The solution should be verified for conformity to the communications specification by a competent authority recognised by the government for this purpose.

Rationale

TC/DRM solutions may require:

- attestation communications, possibly involving non-government systems;
- encrypted traffic entering and leaving government computer systems.

Such communications and other unknown activity can compromise the integrity of government systems and information. Government needs to know enough about what is being sent/received, and the circumstances under which this will happen, to be satisfied that the integrity of government information and related systems will be maintained.

Supports Information Confidentiality and Integrity principles.

Scope & Interpretation

The onus for compliance with this policy will rest with each agency.

Nevertheless, it is recognised that it will be difficult and sometimes impossible for an agency to determine what types of communications may be generated by a particular TC/DRM solution.

Therefore, this policy provides for an agency to require the developer of the technology to document any communications that could affect the integrity of government-held information, and for that documentation to be independently verified.

There are many ways that this verification process could be undertaken, and more work is required to identify the most appropriate ways for this to be done. One possible approach may be through the establishment of an international body, trusted by the New Zealand government (and other governments).

Any such an endeavour will take time and much consultation and cooperation between a wide range of stakeholders before it can be completed.

In the meantime, agencies will need to comply with this policy using 'best efforts' and through establishment of good communication with cooperative providers of the technologies.

It must be made clear, before government adoption of a TC/DRM solution, what the implications may be for a product's functionality if certain communications are opted out of.

System Security Principle

The security of government systems and information must not be undermined by use of trusted computing and digital rights management technologies.

13. Ability to identify harmful communications

Agencies will reject the use of TC/DRM mechanisms, and information encumbered with externally imposed digital restrictions, unless they are able to satisfy themselves that the communications and information are free of harmful content, such as worms and viruses.

Rationale

TC/DRM's use of encrypted traffic challenges the effectiveness of conventional, perimeter-based scanning of incoming data. Government needs to consider whether it has adequate means of protection before using TC/DRM mechanisms, or accepting information with usage restrictions.

Supports System Security priciple.

Scope & Interpretation

Harmful content includes viruses, 'malware' and any other potentially damaging electronic communications or file contents that the agency deems as a risk to the organisation or its data.

Mechanisms to deal with this issue could include:

- the sender assigning rights to an 'organisational user ID' to inspect the communications/ information;
- agency border capability to emulate the intended recipient;
- checking of material on the desktop, if that is the point at which it is decrypted;
- isolating the content to ensure it has no access to other resources;
- trust agreements (most likely to be appropriate when communications are agency to agency).

Glossary

Access

Access refers to the ability to use information. Access has not fully occurred if essential elements of the information's presentation – formatting and layout that in some way contributes to the meaning or usefulness of the information - have not been reconstructed.

Agencies

Agencies in the context of this document are organisations in the executive branch of government, whether at central or local level. 'Agencies' includes contractors and other parties acting on an agency's behalf.

Digital Rights Management

Digital rights management (DRM) is a set of technologies designed to apply and enforce persistent access restrictions to digital information, as specified by the information provider. Digital rights management can regulate the types of actions that can be done with information (for example, view, print, copy or modify) and the time frame in which that information remains accessible.

DRM restrictions may be identity based (e.g. "User A" can view the contents but not modify them) or apply to all users (e.g. the content can be viewed by anyone but only until the end of the month). Other examples include limiting who can view, modify, print or copy the information, when access to the information expires, and what operating platforms the information can be used on.

The restrictions are persistent in the sense that they are designed to be inextricably bound to the information. DRM restrictions are unlike file-system based controls in that they are enforced regardless of the storage method or platform that the information is accessed from.

Examples of information *not* regarded as being DRM-restricted include:

1. Information held in a network file system that restricts access based on an ACL (access control list). If a user has access rights, they can copy the information to a location where the ACL is not enforced.
2. A document held in a DMS (document management system), for which a user with access rights can open the document and save a copy to an unrestricted area outside of the DMS.

In both of the above examples, the restrictions are not inextricably bound to the information. When the information is moved from the system in which it is stored, the restrictions do not persist.

Mere encryption of information (e.g. encrypted emails) is not deemed to constitute DRM. It is only when decryption depends on software that enforces any form of access restrictions (e.g. prevents modification of the contents, or copying or saving of the unencrypted information) that DRM is deemed to be applied.

Encumbrance

‘Encumbrance’ refers to restrictions on the rights to use information.

Information

For the purposes of this document, ‘information’ is deemed to include data.

Integrity

For the purposes of this document, “integrity” is used in the wider sense of the word, meaning, “the state of being unimpaired; soundness” (source: The American Heritage Dictionary of the English Language, Fourth Edition). This definition therefore includes qualities such as availability and confidentiality. It is not limited to the narrower technical meaning of assurance that information has not been altered or destroyed in an unauthorised manner.

Public Business

“Public Business” refers to any activity carried on by a government agency, in accordance with its statutory or other government-directed responsibilities.

Restrictions

Limitations on access to information, enforced through technology, e.g. copying prevented.

Rights

Generally refers to the particular types of access granted to information when access to the information has been restricted through the use of TC/DRM encumbrances.

Solution

A combination of people, processes and technologies to satisfy a business need. It may consist of more than one system.

TC/DRM

Trusted computing and/or digital rights management, functioning separately or working together.

Trusted Computing

There is much debate amongst experts and informed commentators about the definition for "trusted computing". The following definition - used for the purposes of these principles and policies - seeks to incorporate wording about which there is general (but not necessarily universal) agreement.

Trusted computing is a combination of software and hardware supporting applications to ensure that data cannot be accessed unless the user's system is operating as expected and has not been tampered with.

Trusted computing entails some or all of the following capabilities:

- Process isolation, so that one process cannot access the memory of another.
- Data encryption, key storage and other cryptographic functions.
- Secure paths between the secure processing area and the keyboard and video display.
- Attestation, a mechanism for validating aspects of the software and hardware configuration locally or across a network.

Trusted computing also generally includes a unique public key pair and certificate chain, bound to the computer, so that the computer can be identified and authenticated.

Trusted computing architecture could be implemented in a range of ways, and one example of this would be based on the specifications of the Trusted Computing Group (TCG). A key element of the TCG architecture is the Trusted Platform Module (TPM), a specialised chip containing the cryptographic keys, access to protected storage and the functions to measure and attest to the computer's integrity and trustworthiness.