TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 35: Implementing Information Security

Part 4 Information Security Policy

An Information Security policy serves as the foundation for information security management within an agency. The development of this policy is the first step in establishing management commitment, and documenting responsibilities for information security within the agency and should therefore be concise and clear. This advice provides a step by step approach to developing an information security Policy. This is a more detailed guide to Step 9 and 10 in advice 35 part 1 Implementing Information Security.

The Information Security Policy – Mandatory Clauses template has been developed to assist agencies in the development of an information security policy and details the minimum set of mandatory requirements and quality criteria that must be included. It also makes suggestions for agency specific considerations. See attached Template.

What this advice is about

This advice is one of a series issued by TAHO produced to support good practice in information security.

It explains why an information security policy is important, how it should be developed and issued, and expands on the guidance in the WoG Information Security Policy Manual.

The advice is arranged in the following sections:

1. Purpose and scope of the information security policy

2. How to write an information security policy

3. Issuing and implementing the information security policy

4. Managing Issues

5. Reviewing the Information security policy

1. Purpose and Scope of the Information Security Policy

An Information security policy should fulfil many purposes. It should:

- Protect people and information
- Demonstrate to employees and stakeholders that managing information security is important to the agency
- Serve as a mandate for the activities of the information security manager/officer
- Set the rules for expected behaviour by all agency staff, system administrators, management, senior management, security personnel, volunteers
- Authorize security personnel to monitor, probe, and investigate
- Define and authorize the consequences of information security breaches
- Define the Agency consensus baseline stance on security
- Help minimize risk
- Provide a framework for supporting documents such as procedures, business rules, etc.
- Help track compliance with WoG Policy and legislation

Information security policies provide a framework for best practice that can be followed by all employees. They help to ensure risk is minimized and that any security incidents are effectively responded to.

Information security policy development will help to define the Agency information assets, and will also help turn staff into participants in Agency efforts to secure these assets. Information security policy defines the organization's attitude to information, and announces internally and externally that information is an asset, the property of the organization, and is to be protected from unauthorized access, modification, disclosure, and destruction.

Policy should be used by the agency as a catalyst for change. It is possible to use the policy to drive the agency IS project initiative, with the policy as the catalyst for future projects to move towards better information security practices. For example, a policy stating that a certain type of encryption is required for sensitive information sent by email may (with prior consultation with the appropriate technical experts) help to promote the need to develop such a capacity in the future. The presence of this requirement in policy has made sure the impetus to develop the email encryption project has remained strong. In short, security policy should be a useful tool for protecting the security of the Enterprise, something that all users can turn to in their day-to-day work, as a guide and information source.

Top tip

- ➢ Keep the policy short – leave details of how information security is to be managed and instructions to staff to supporting documents (unless your organisation's policies habitually contain this level of detail).

2. How to write an Information Security Policy

This section of the guide outlines a series of steps to follow in developing the information security policy.

- **Step 1: Establish Senior Management Support**
- **Step 2: Research the Agencies current Information Security Management Practices, Resources and Attitudes**
- **Step 3: Consult staff and Identify your Audience**
- **Step 4: Look at other Information Security Policies**
- **Step 5 Determine Policy Structure**
- **Step 6: Identify Who Will Need to be Involved – The Policy Development Team**
- **Step 7: Identify Related Policies**
- **Step 8: The Policy Development Process**
- **Step 9: Write the Initial Draft**

Step 1: Establish Senior Management Support

Developing a suite of policy documents will require a high level of commitment, not just from the Information Security committee but also from a number of other information security personnel in the agency. In order to make sure that these resources are readily available to you in order to acquire the information you need, management buy-in must be sought at the beginning of the policy project. Management must be made aware of both the importance and size of the task ahead, so that they will not baulk at resource allocation in the later stages.

The key to ensuring that your agency's security policy is useful and useable is to develop a suite of policy documents that match your audience, and marry with existing company policies. Policies must be useable, workable and realistic. It is essential to involve and get buy-in from major players in policy development and support (such as senior management, audit and legal) as well as from those people who will have to use the policies as part of their daily work (such as subject matter experts, system administrators and end users).

A key element to success is to communicate the importance and usefulness of policies to those who have to live by them. Often staff seem to think that policy is something that is going to stand in the way of their daily work. An important element of policy development, and to ensure policies are put into practice and not rejected by staff, is to convey the message that policies are useful: to provide a framework within which they can work, a reference for best practice and to ensure staff comply with legal requirements.

Once staff realise that policy is something that may actually help them as they go about their work, they are much more likely to be receptive to both helping you develop it and living up to it to ensure compliance. Similarly, once senior management realise that policy is a tool they can leverage to help ensure adherence to legislative requirements, and to move forward much needed new initiatives, they are much more likely to be supportive of policy in terms of financial and resourcing support.

Senior management also supports the policy development and maintenance process by championing the resulting policies throughout the agency and putting their weight behind them so that the policy is seen to have "teeth". Further, they should be prepared to support projects that result from policy to ensure compliance. These two types of support are essential to the ongoing viability of the policy program.

Top tips

- ➢ Tap into relevant organisational agenda and initiatives.
- ➢ Explain the importance of a policy as an initial platform for improvement in information security practices.
- ➢ Suggest that issuing a new policy will offer a 'quick win' for information security work.

Step 2: Research the Agencies' current Information Security Management Practices, Resources and Attitudes

If you do not already know what your agency's information security practices are, you need to investigate them and identify any gaps. This will help you to establish the new policy's content, priorities and emphasis. At this stage you should be in a position to assess the corporate culture and whether it is on balance supportive of, or resistant to, information security. The question of resources for the information security function will also be relevant. The policy should be realistic and achievable given the organisational culture and available resources.

If your agency has any existing security policy, review it to determine if it can be used as part of the new suite of policy documents. Collect all related procedures and guidelines as well as any high level policy documents. These can all be used to get an idea of the current agency stance on a given issue or technology, or simply to show that a certain technology is secured differently in different areas of the agency. This is something that will need to be reflected in the new policy document. Even existing guidelines or job aids can become the starting point for a policy document on the same topic. See Part 1 of this advice 35 for a gap analysis template.

Step 3: Consult Staff and Identify your Audience

It is important to establish staff views on information security management in general, and a policy in particular. Staff will have useful insights into corporate culture as well as current practices which should inform the policy and related procedures.

Top tip

- Consultation now will make it easier to secure buy-in later, because staff will feel their views and concerns were taken into account.

Your audience is of course all your Agency employees, but this group can be divided into audience sub-categories, with the members of each sub-category likely to look for different things from information security policy. The main audience groups are:

- Management – all levels
- Technical Staff – systems administrators, etc.
- General Agency staff (including volunteers)

All users will fall into at least one category (general agency staff) and some will fall into two or even all three.

The audience for the policy will determine what is included in each policy document. For example, you may not always want to include a description of why something is necessary in a policy - if your reader is a technical custodian and responsible for configuring the system they are likely to already know why that particular action needs to be carried out.

Similarly, a manager is unlikely to be concerned with the technicalities of why something is done, but they may want the high-level overview or the governing principle behind the action. However, if your reader is agency staff, it may be helpful to incorporate a description of why a particular security control is necessary because this will not only aid their understanding, but will also make them more likely to comply with the policy.

Allow for the fact that your readers will want to use the policies in a number of ways, possibly even in more than one way at one time. For example, when first reading a policy document, agency staff may be interested in reading the entire document to learn about everything that they need to do to help protect the security of the agency. On another later occasion however, the user may reference the document to check the exact wording of a single policy statement on a particular topic.

Given the variety of issues, readers, and uses for policy, how can we hope to address them in one document? The answer is that we can't. Agencies must ensure that their information security policy documents are coherent with audience needs and to do this it is often necessary to use a number of different document types within a policy framework. Which type of document you use will be determined in large part by the audience for that document. For example, an overall Acceptable Use Policy will be in the form of a higher level document, while a document that describes how to configure the instant messaging system to ensure it complies with the Acceptable Use Policy may be in the form of a technical procedure or guidelines document. Managers and agency staff are likely to be interested in the former, while administrative staff are more likely to use the latter. See the Tasmanian Project Management Guidelines for further advice on identifying stakeholders.

Step 4: Look at other policies

Examples of Information Security Policy from other organisations – particularly those in the same sector – can be a useful starting point.

Top tips

- Use good examples from other organisation's policies. But adjust them as necessary to ensure your Information Security policy has the right corporate look and feel.

Step 5: Determine Policy Structure

A policy is an expression of intent. A written policy is the primary means by which a board or executive team gives direction to management and staff, and informs other stakeholders. Effective security policies provide clear direction and commitment, and establish clear roles and responsibilities. Policy is part of effective corporate governance.

Information security policies provide executive direction and support, and establish operating plans and processes. Policies establish the required behaviours and outcomes, and may vary widely in their specificity. There are no hard and fast rules to define the format or content of information security policies.

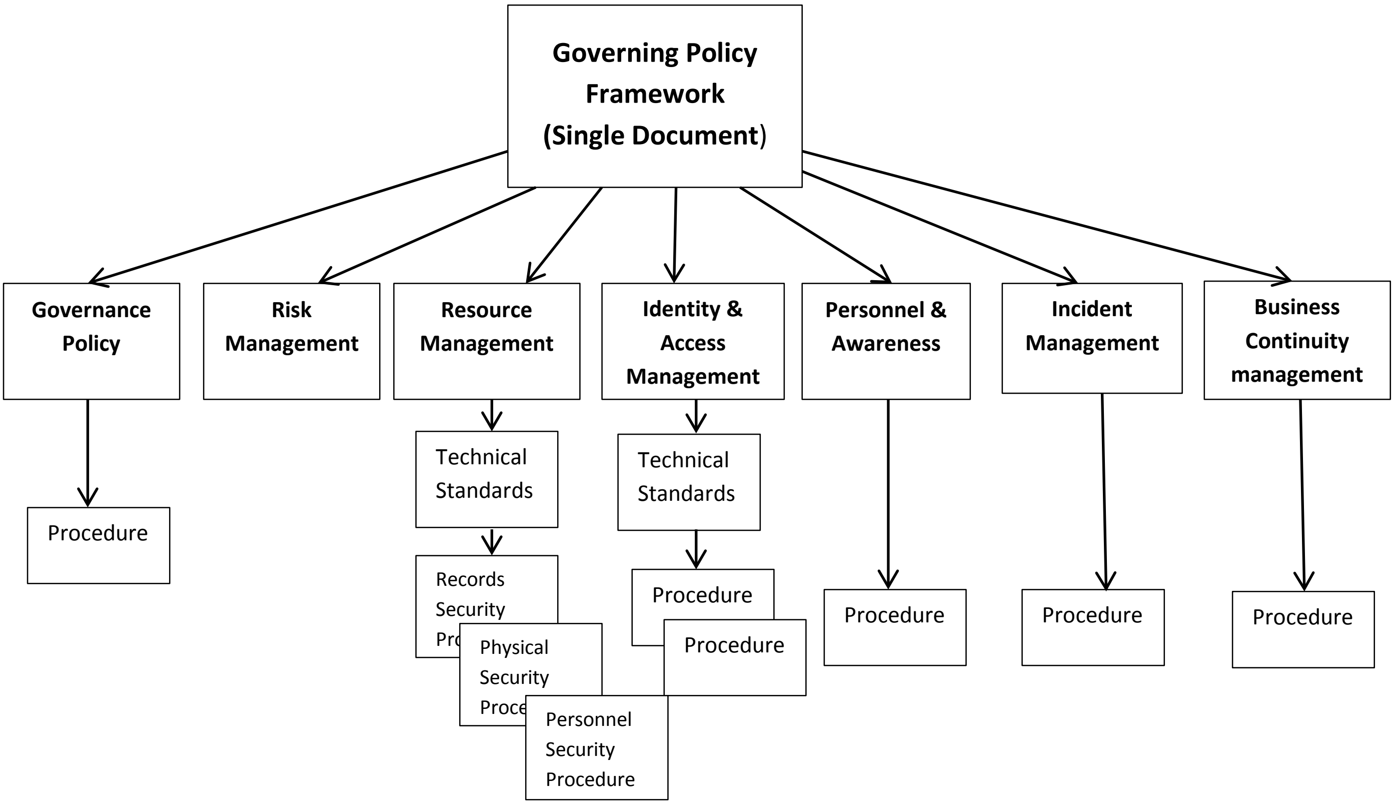
The size and shape of information security policies may vary widely from Agency to Agency. This may depend on many factors, including the size of the agency, the sensitivity of the business information they manage, and the numbers and types of information and computing systems they use. For large Agencies, developing a single policy document that speaks to all staff within the agency and addresses all the information security issues necessary may prove impossible. A more effective concept is to develop a suite of policy documents to cover all information security bases; these can be targeted for specific audiences, making a more efficient process for everyone.

It should be noted that there is no single method for developing a security policy or policies. Another factor to be considered is the maturity of the policy development process currently in place. An Agency which currently has no information security policy or only a very basic one may initially use a different strategy to an Agency which already has a substantial policy framework in place, but wants to tighten it up and start to use policy for more complex purposes, such as to track compliance with legislation.

When starting out it is a good idea to use a phased approach, starting with a basic policy framework, incorporating the major policies that are needed. Over time, additional supporting policies can be developed, including refining/revising those that are already in place and adding to this through the development of accompanying procedures and planning documents.

Policy Hierarchy Overview

The diagram below outlines a hierarchical policy structure that enables all policy audiences to be addressed efficiently. This is a template for a policy hierarchy and is based on the mandatory requirements of the Tasmanian Government Information Security Policy Manual. It can be customized to suit the requirements of any agency:



The diagram above shows a hierarchy for a fairly mature, developed process, probably aligned to that possible in a large agency where policy development has been underway for several years. For smaller agencies or for those just starting to develop policy, it is possible to use this basic framework, but to initially have a smaller number of Technical Standards and leave guidelines or procedures until later in the process. Rather than trying to develop a large hierarchy all at once, it is more realistic to develop a Governing Policy and a small number of Technical standards initially, then increase the number of policies and supporting documents, as well as the complexity of the policies, as you move forward.

In large agencies there will be several audiences for your policy, and you will want to cover many different topics on different levels. For this reason, a suite of policy documents rather than a single policy document works better in a large agency environment. The hierarchical structure of the suite of security policy documents reflects the hierarchical structure of roles in a large agency. The proposed scheme provides for all levels of audience and for all topics by using two policy types supported by procedural documents:

- Governing Policy Framework
- Technical Standards
- Procedures

Governing Policy

Governing Policy should cover information security concepts at a high level, define these concepts, describe why they are important, and detail the agency's stance on each. Governing Policy will be read by managers and staff. By default it will also be read by technical custodians (particularly security technical custodians) because they are also staff. All these groups will use the policy to gain a sense of the agency's overall security policy philosophy. This can be used to inform information security-related interaction with business units throughout the agency.

Governing Policy should be closely aligned with existing and future Human Resources and other agency policies, particularly any which mention security related issues such as email or computer use, etc. The Governing Policy document will be on the same level as these agency-wide policies.

Governing Policy is supported by Technical Standards which cover topics in more depth, providing specific detail for every relevant technology. Covering some topics at the Governing Policy level may help avoid the need for a detailed technical standard on these issues. For example, stating within the agencies governing password policy that details of specific password controls can be covered for each operating system or application in the relevant technical standard, means that a technical standard on password controls for all systems is not required. This may not be the case for a smaller agency, where fewer systems/applications are used and where a single technical password standard would therefore be sufficient. For a larger agency however, the former method provides a more efficient process for staff to follow because they will have to reference fewer documents – simplifying this process raises the odds that staff will comply with the policy, thereby improving security.

In terms of detail level, governing policy should address the "what" in terms of security policy.

Technical Standards

Technical Standards will be used by technical custodians as they carry out their security responsibilities for the system they work with. They will be more detailed than Governing Policy and will be system or issue specific, e.g., a Physical Security Technical Standard or a Database Security Technical Standard.

Technical Standards will cover many of the same topics as Governing Policy, as well as some additional topics specific to the overall technical topic. They are the handbook for how an operating system or a network device should be secured. They describe what must be done, but not how to do it - this is reserved for procedural documents which are the next detail level down from Governing and Technical Standards.

In terms of detail level, Technical Standards should address the "what" (in more detail), "who", "when", and "where" in terms of security policy.

Procedures

Procedural documents give step-by-step directions on the 'how' of carrying out the policy statements. For example, a guide to hardening a Windows server may be one of several supporting documents to a Windows Technical Standard.

Procedures are an adjunct to policy, and they should be written at the next level of granularity, describing how something should be done. They provide systematic practical information about how to implement the requirements set out in policy documents and Technical Standards. These will be written by a variety of groups throughout the agency, and may or may not be referenced in the relevant policy, depending on requirements.

Procedural documents may be written in addition to, and in support of, the other types of policy documents, to aid readers in understanding what is meant in policy through extended explanations. Not all policies will require supporting documents. Beware however, if you find yourself getting requests for procedures for every policy document you write, your original documents may be too complex. Save your own and your readers time, by ensuring everything you write is clear, concise, and understandable in the first place.

The development of these supporting documents need not necessarily be undertaken by the policy development team who develop the Governing and Technical standards. It may be more efficient to have the individual business unit develop their own supporting documents as needed, both because of the availability of resources on the policy development team and because the technical staff in the business units are likely to have the most complete and up to-date technical knowledge in the agency, better enabling them to write such documents.

The policy provides the framework to follow (the "what", "who", "when", and "where" in terms of security policy) and technical staff simply need to follow these controls and sketch out the "how".

Procedures will also act as a backup facility if a staff member leaves, ensuring their knowledge isn't lost and that policy requirements can still be carried out.

Policy topics

Prioritizing Policy Topics

When you begin to write security policy you will need to prioritize what topics need to be addressed first. A number of factors should be taken into account during this process. First, look at any areas containing information that you are legally obliged to protect. These areas will be defined (although not always clearly) in National, State, or Local government legislation. Secondly, look at information that may be used in critical decision-making by your agency or your clients. You may also be legally liable for compromises to the confidentiality or integrity of this information. The risk analysis you have undertaken will indicate where policy priorities are.

The remaining information should be prioritized according to business criticality and sensitivity, that is, how critical the information is to the continuation of your agency business processes and how much damage would result from unauthorized disclosure of the information. This will enable you to see which information is more sensitive.

Outline Policy Topic List

When you have prioritized your information using the guidelines above, you can then begin to break it down by area into separate policy documents. Divide your topics by issue, system, application, technology and general. You are then ready to determine which topics you need to reference in Governing Policy and which also need a separate technical standard.

Governing Policy

Governing Policy should cover all aspects of security at a higher, broader level than the detail contained in the Technical Policies. All major security topics need to be covered. This is the place to state the agencies' baseline stance on these issues.

When first developing a Governing Policy (where none previously existed), the main concern may be to cover the main topics, while subsequent revisions may incorporate more company-specific topics as feedback is received and the policy development team gains familiarity with what issues need to be addressed. The Information Security Policy – Mandatory Clauses template which accompanies this Advice provides a template for agencies to use when developing a Governing Policy

Technical Standards

The number of Technical Standards required will depend on the number of operating systems, applications, and other technologies used by your agency. Listed in the template that accompanies this advice are some categories that can be used to identify policy needs in each area. Each entry in a category represents a single Technical Standard document. This is by no means an exhaustive list, and while the list for any given agency will be dictated by the technologies in use by the agency, some standards will be almost universal and most agencies will need to consider developing a standard for these areas. This may seem like a large number of standards, but remember that the audience for these documents are technical people who work specifically with these technologies. Therefore, most technical staff will only have to read and know about the content of one or two technical standards.

Another way of structuring technical information security standards is to group by security topic, e.g., one standard on authorization, another on authentication, another on securing sensitive information, etc. There are times when this works well (physical security, privacy) and times when it isn't so successful (authentication, authorization), particularly for agencies whose policy development model hasn't reached full maturity.

The agencies baseline stance on authentication fits comfortably into the Governing Policy for example, but when it comes to the detail on authentication (differences between platforms, etc.) this is best tackled in the Technical standard for as many technologies as need it, rather than in a single authentication standard.

The reason for this is clear if you think again about how staff are likely to use the standard. Most users who need more detail than is contained in the Governing Policy will be searching for policy statements on a given technology ("I need to secure this Windows server, can you point me to the correct standard, please") rather than on a given topic. Therefore they would not welcome having to search through standards on authentication, authorization and auditing to find out how to configure a given operating system or application.

The list of policy categories that is in the accompanying Policy Template is a sample list of some of the policies, technical standards and procedures an agency might expect to develop. Note however that the universal list is virtually endless, and therefore each company's list will be different. Depending on how your agency is set up, you may also group these standards differently, for example it may make sense to include your standard statement on VPN in your Remote Access Technical Policy in some cases. Another agency might decide to have a single Technical Policy dealing with all peripheral devices while a larger agency which uses many types of these devices might decide to have several standards dealing with individual device types.

Procedures

The list of procedural documents an agency might need is perhaps even more varied than the technical standards list. As these may be developed based on policy by individual business units rather than by the policy development team, in a large agency you may not even know how many are out there. In other circumstances the policy development team will assist with the development of these documents.

An example of procedural documents are Disaster Recovery Procedures. These will describe the process for developing and maintaining a Disaster recovery plan, including details such as roles and responsibilities of who owns the plan, who has the ability to update it, etc. In addition, the guidelines could list the required plan elements and how often the plan should be tested. See the Template for the Governing Policy which accompanies this advice.

An Agency Example – Information Security Policy Framework

The framework states why information security is important, defines what has to be done to secure communications and information technology resources, how security rules are to be implemented and who is responsible for their implementation.

Framework element	Purpose and content	Role Responsible for Approval
Policies	Information security policies are the high level mandatory rules that state why information security is important and define the objectives and strategies for protecting the confidentiality, integrity and availability of CIT resources.	Commissioner/Secretary
Guidelines	Guidelines contain detailed security requirements and criteria for meeting information security policy objectives and strategies.	Deputy Commissioner
Technical Standards	Technical Standards contain detailed security requirements and criteria for meeting guidelines and policy objectives. Technical Standards may incorporate information security checklists.	Director Corporate Services or relevant Commander
Procedures	Procedures explain in detail how the security requirements are to be implemented.	Managers and Officers in Charge

Information security policy categories

The information security plan framework is built around the following policy categories.

No.	Category	Objective
1.	Information security governance	Define roles and responsibilities within the Agency for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security.
2.	Record security	To ensure that controls are established to achieve best practice record keeping to protect the creation, preservation, disposal, transfer, release and access to Agency Government records
3.	Information security classification system	To ensure that official information is protected commensurate with the consequences of unauthorised disclosure, misuse or compromise.
4.	Physical security	To ensure that controls are in place to protect the physical security of all communication and information technology resources. The level and types of controls implemented should minimise the risk of equipment or information being rendered inoperable or inaccessible, or accessed or removed without appropriate authorisation.

No.	Category	Objective
5.	Asset control	To ensure that security-classified Agency communication and information technology resources are identified and recorded in registers so that responsibility can be assigned for maintaining appropriate security controls.
6.	Personnel security	To ensure that employees, contractors and third parties understand their responsibilities and are suitable for the roles they are considered for and to reduce the risk of theft, fraud or misuse of Agency information and CIT facilities.
7.	Information facilities and systems operations Management	To ensure that security controls must be in place to safeguard all operations of Agency information facilities and systems.
8.	Database security	To control and co-ordinate the use of Agency local and corporate database systems and related data. What is this?
9.	Network and communications management	To ensure that security controls are established to protect Agency networks and infrastructures from unauthorised access and to safeguard information confidentiality and integrity.
10.	Security of computerised communication systems	To prevent the loss, modification or misuse of Agency data, stored or transmitted on computerised communications systems.
11.	Electronic information transfer	To ensure that appropriate security controls are in place to protected information when being transferred electronically
12.	Access control management	To prevent unauthorised computer access.
13.	Security audit logging	To ensure that information related to security relevant activities is recognised, recorded, stored and analysed in order to minimise future security incidents and to provide evidence of past security incidents.
14.	Information Systems acquisition, development and maintenance	To define security requirements of information systems during all stages of the information system life cycle.
15.	Business continuity management	To have business continuity plans available to counteract interruptions to Agency information systems and business activities from the effects of major failures or disasters.
16.	Information technology media handling and Management	To prevent unauthorised use, disclosure, modification, removal or destruction of fixed and removable information technology media
17.	Cryptography	To ensure that approved cryptographic systems and techniques are used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

No.	Category	Objective
18.	Malicious and mobile code control	To protect the integrity of Agency software, data and information from the threat of computer malicious code and unauthorised mobile code infection.
19.	Monitoring for Compliance	To define requirements for monitoring use of information processing facilities in accordance with Agency policy, statutory law, common law, international law and contractual requirements.
20.	Information security incidents	To ensure that effective processes are established for detecting, reporting, recording and resolving information security incidents.
21	Information Security Risk Management	Regular risk assessments and system audits should be conducted to ensure the security of Communication and Information Technology (CIT) resources.

Step 6 Identify Who Will Need to be Involved – The Policy Development Team

Determine Resource Involvement

At this point you should identify who you will need to talk to in order to determine and agree on the content of the policy. You must give all team members an estimate of how much of their time they can expect to allocate to the project. Policy projects held up because subject-matter experts (SMEs) are busy can mean that the policy risks being obsolete before it is finished. If necessary, get buy-in directly from line managers. In most cases, people will see the value of policy and will be happy to help you develop something that will help them in their jobs, but you need to make sure they are on board before going any further.

The overall composition of the policy development team will vary according to the policy document being developed, but the following is a list of individuals or groups who may be involved.

Agency staff with involvement in the development of the IS policy suite included:

- Chief Information Officer
- Deputy Secretary or Manager Corporate Services
- All Corporate Services Directors (ICT, HR, Facilities, and Information Management)
  Note: The Human Resources department may need to review and/or approve your policy depending on how you have determined that your policy will relate to existing agency policies. Where your policy touches on topics covered by existing HR policy, e.g., email usage, physical security, you must make sure that both sets of policy say the same thing.
- Information Security Officer or Project Manager for the agency
- Managers of functional business areas of the department (divisions or business units other than corporate services)
- Legal and Risk Managers
- Technical Personnel –you will need to call upon the expertise of technical staff who have specific security and/or technical knowledge in the area of the technical standards that need to be developed. They will be familiar with

the day-to-day use of the technology or system and are the best placed person to develop the technical standard.

- Audit – The Internal Audit department in your company are likely to be involved in monitoring company-wide compliance with the policy once it is in force. It is therefore useful if they are involved in the development and review processes for policy, to ensure that it is enforceable in terms of their procedures and current best practice. If there are other compliance groups additional to the main internal audit department, these groups should also be consulted as needed.
- Staff – During revision of policy documents, it can be useful to work with users to determine how successful current policy is, and thereby determine how the policy may need to be changed to make it more useable for your target audience. Issues such as the style, layout, and wording of your policy documents may seem minor issues compared to their content, but remember that if your documents are off-putting or hard to understand, users may not read them fully or may fail to understand them correctly, thereby needlessly risking security compromise.

These people will be assigned the overall responsibility for developing the policy/technical standards documents. Overall control may be given to one person with others in a supporting role. This team will guide each policy/technical standard document through development and revision and should subsequently be available to answer questions and consult on the policy.

Step 7: Identify Related Policies

Many organisations will have a collection of policies that the Information Security policy should complement and refer to. It is important to locate and research these other policies to ensure a coherent policy framework.

TAHO have released an Advice on *Developing and Information Management Policy (2013: Advice 50)* This includes a sample policy template and is available on our website.

Examples of Related Policies:

- Data protection
- Information Management
- Business continuity
- Risk management
- Right to Information (RTI)
- Email
- Acceptable use
- Personal Information Protection

Step 8: The Policy Development Process

The major consideration behind any Agencies policy development process will be the level of process maturity. It is important that Agencies (especially larger ones) don't aim too high initially and try to develop a comprehensive and complex policy program straight away. This isn't likely to be successful for a number of reasons including lack of management buy-in, unprepared Agency culture and resources, and other requirements not in place. In this situation it is advisable to start off small, perhaps developing checklist–style policies initially and only implementing a skeleton policy framework, with essential policies developed first.

As the process grows in maturity, Agencies will be able to further develop the full range of policies as well as Agency technical standards and procedural documentation as needed. Awareness raising and communication processes will also grow in maturity to cope with promoting an ever-growing range of policies. This should coincide with the growing corporate strength of the policies themselves. The Agency culture will start to appreciate that the policies must be followed and may actually start to use them to push through much needed changes throughout the agency.

The best policy will come from a combination of these approaches, both top-down and bottom-up. This is something that must be considered from the outset and must be reflected in the diversity of areas involved in policy development and the types of review policy undergoes.

This balanced approach is likely to result in a more mature policy development process. It can work for both small agencies (where there is little space between top and bottom) and big agencies where the breadth of knowledge is needed to ensure a realistic and workable resulting policy.

Step 9 Write Initial Draft

Determining the right pitch or level for the policy can make the difference between a feasible security policy and one that is merely shelf-ware. Make the policy too rigid and it will be unenforceable, but make it too weak and it will provide insufficient protection. Be aware that there may well be exceptions to some of the policy statements. In these cases, it is acceptable to leave the statements in the policy, but to refer the exceptions in the deviations process. This ensures that the agency policy is clearly stated and enforced according to risk assessment and best practices, while at the same time providing a mechanism for dealing with occasional exceptions without weakening the policy.

Even if you don’t have fully formed policy statements at this point, it is a good idea to get something down on paper before your first review meeting with the rest of the project team. Even a list of topic headings and questions is easier to work from than a blank page.

Style considerations

The following style guidelines will help to ensure your policies are useable:

- Consult your corporate style guide. If one exists, this will be an easy way to ensure all your policies have the same look and feel and will also help them to be more quickly accepted as corporate documents. If you don’t have a style guide, consider developing one to ensure consistency throughout your policies. This will also make them easier to update and review.
- Ensure you have a consistent writing style throughout. There is much debate about the passive voice versus the active voice; whichever you use, chose one and stick to it throughout to aid comprehension.
- Be clear and use concrete rather than abstract language, e.g., say “log files must be reviewed at a minimum annually” rather than “log files must be reviewed regularly”. What is considered “regular” will differ from person to person and your policy must mean the same to everyone so that it can be applied consistently.
- Use plain English. All your readers must be able to understand your policy, and they shouldn’t have to wade through reams of information to get to the point.
- Don’t include anything that isn’t policy in the policy statements section of the document. Background information, for example, should go in a section of its own, either at the start of the document or in an appendix. You will weaken your policy statements by mixing them with informational statements. Similarly, procedural information should go in separate guidelines documents.

Review with Additional Stakeholders

During the review phase the policy should be reviewed by any groups who have an interest in the policy. This includes any groups who will be expected to work with the policy, who may have knowledge that needs to be taken into account when developing the policy, or who are able to help ensure that the policy is enforceable and effective. Such groups include the Legal and internal audit units. In addition, regional offices should be considered here, they will have to comply with the policy, but their requirements may be different from those of the central office and this should be considered in the review phase.

Policy Gap Identification Process

Before publishing policy, it is a good idea to determine which (if any) policy statements are not currently in force in your agency. These are known as gaps. The Information security committee will endorse a policy/technical procedure work program to close the gaps, which will need to include identified positions who will be responsible for writing or coordinating the development of these documents.

Once you have identified any gaps, it is a good idea to keep a record of the gaps for each policy somewhere in a project plan. This should be regularly submitted to the Information security steering committee in your agency to monitor progress of the policy development project. This record will also be a useful resource when you come to revise the policy in the future.

3 Issuing and Implementing the Information Security Policy

This section of the guide suggests some approaches to issuing and implementing the policy. It is not prescriptive because agencies differ and what works in one might not work in another. This section covers:

- Developing a Communication Strategy
- Senior management endorsement
- Issuing and implementing the policy
- Making the policy available, internally and externally
- Activate a Communication Strategy

Developing a Communication Strategy

Although once implemented the policy will be constantly available, you will initially need to make agency staff aware of new or updated policy. Develop a communications strategy and have it approved by the Agency Information Security Committee. You may like to work with your Communications unit to do this. Ensure that all appropriate management groups are informed, so that they can filter down information in their area.

It stands to reason that if policy is not read it will not be adhered to, so don’t underestimate the importance of successfully communicating new policies to the various audience groups. Depending on the size of the agency and the maturity of the policy development process, this will be more or less complex. Smaller agencies have an easier job in that it is logistically easier for them to reach all employees and let them know what they should be reading and following. It is also likely that smaller agencies will have fewer policies for their employees to read since they will usually have fewer technologies in use.

However, even getting employees to read the Governing Policy can be a challenge, especially existing employees when the policy changes. Here are a few suggestions for how to tackle this:

- Include adherence to IS Policy in the agency Statements of Duties.
- Make policy part of required training: incorporating information security policies into a training course (or courses) and making it a requirement for employees to complete these courses annually is another way to ensure policies get read and hopefully adhered to following course completion.

Senior Management Endorsement

Senior management support is a critical success factor. The policy should be clearly endorsed by senior management in the same way as other significant policies of the agency. There are several options, depending on the agencies usual practice:

- the policy could include a statement that is has been formally approved by the secretary/CEO of the department
- the policy could be issued in a way that makes it clear to all staff that it is an official approved policy that should be taken seriously – i.e. issued by the agencies secretary or CEO.

Issuing and Implementing the Policy

Implementing a new policy requires thorough planning. There may be resistance to change within the agency and the benefits of new arrangements may need to be explained and sold to staff. Implementation strategies include:

- initial and continuing publicity
- ensuring related procedures and guidance are in place (and the timeframe for the development of new ones is communicated clearly)
- emphasising senior management endorsement
- being visible and accessible, e.g. visiting each part of the organisation in turn
- monitoring and reporting

Ideally, there will be a formal launch of the policy with internal publicity which draws it to the attention of staff and makes it clear to them that adherence to its provisions is mandatory. Most agencies have standard arrangements for informing staff of things they need to know, such as memos circulated to all staff or news items on their internal website. The Project Manager or chair of the IS committee should also present the policy at business unit or divisional meetings.

Which option is chosen will depend on what works best in your agency. However, it should be made clear that the policy is part of a wider programme and accompanies - or will be followed shortly by - supporting policies/technical standards and procedures, and briefings or training sessions.

Policy documents should be published so that they are available to all agency employees. This usually means putting them on an agency intranet site, possibly the Information Security team's own intranet site.

Activate Communication Strategy

Email is probably the best way to inform employees about policy changes quickly and effectively, although you may also want to include information about policy in other forms of company communication, and through your agency's security awareness program.

Ensure policy is reflected in awareness strategies. An effective security awareness strategy will ensure that all your audiences are aware of your security policies, know where to find them and how to comply with them, as well as the consequences of non-compliance. Through a security awareness program, it should be possible to teach policy stakeholders about the policy and their role in maintaining it. This will help make the policy an integral part of their jobs.

It is through using communication and education programs that you will be better able to foster a positive attitude in your agency towards information security. There is evidence to show that users of the information security systems would be more willing to adhere to better security practices if they were knowledgeable (i.e., better trained and better informed) about what good practice actually involved.

A major part of ensuring policies have value is to ensure the employees who are supposed to follow them are aware of them and perhaps even more importantly, are aware of the value of adhering to them. This can be a big cultural shift in any agency. What security awareness campaigns must reflect is that the agency has changed and it isn't about protecting the information just 'well enough' so that it can be used for whatever purpose the agency needs it for. It isn't enough just to do things as they have always been done. This may have been enough previously, but what your security awareness campaigns need to reflect is that things have changed and the front line in ensuring information is protected are the employees.

Once employees realize that even relatively small security breaches can have potentially devastating (and job jeopardizing) consequences, they are much more likely to be willing to act as your first line of defence and to pick up your policies and start adhering to them. Awareness, education and policy go hand in hand, each strengthening the other.

Top tips

- Make sure all new staff, including temporary staff and consultants, read the policy.
- Remind staff of its provisions occasionally. Offer refresher training, write articles for the staff magazine and include news items on the internal website.

4. Managing Issues

This section details some of the things that go wrong during policy development and some ideas to remedy these problems.

Policies Lack Weight

It is a big concern when policies that have taken time and effort to develop are not taken seriously. This is common when starting to develop information security policies and for those whose development process isn't yet mature. Don't worry too much at these early stages. Weight is likely to come with time and increasing numbers of policies, backed up and promoted by a combination of management backing and a good awareness/communication strategy. With this will come a realisation on the part of the agency (and particularly those bodies involved in compliance and governance) that policy can be used to leverage change and a move towards best practice and compliance.

Lack of Reviewing Feedback

Lack of feedback following reviews can also be a fairly common complaint from the policy development team. This is fine if the reviewers have read the policy and simply don't have any feedback; the problem arises when they have skimmed over the document without reading it closely or taking in the implication of its content. In these cases problems may only be noticed at a much later stage or, even worse, after publication. This can serve to weaken the policy and even discredit the policy development process as a whole.

One solution is to review each document in detail at a meeting (or meetings) with each group of reviewer(s). The development team representative can read through each policy statement and seek feedback on each one. This will help make sure the reviewers have both read and thought about the policy in detail.

Sometimes reviewers may not be sure what is required of them and this may result in a low level of feedback. To avoid this, inform all your reviewers about the process and what is expected of them (e.g., you are looking for feedback on the technical content of the policy rather than on typos and grammatical errors).

Another possible reason for this is simply not giving the reviewers enough time to review. Be aware of their workload and agree a realistic timescale in advance. If you are dealing with review groups regularly for more than one policy, agree to a regular timescale and stick to this.

Resources Shortage

This is frequently caused by two things: lack of management support and genuine resource shortages due to high workloads and cost cuttings exercises. If you really can't get access to those people you need to for writing the policy, consider putting it on hold until the resources are available. Report this to the Information Security Committee, and point out that the agency will be without the policy until resources can be found. This may change their mind or they may decide that other things take priority.

Reviews are Slow and Cumbersome

Sometime reviewing policy can seem to go for a long time. This can be because the project team size is too large. The optimum size for the core team is around 3 people. 2-4 is fine but any more than 4 and you start to have to take a lot longer to air everyone's views on each policy statement. If there are other people who are keen to be involved, keep the project team small but have the additional people review the policy as an external stakeholder in a review period of their own. This way not everyone has to be consulted every step of the way but everyone still has input.

Another reason for slow reviews is that often no one wants to take responsibility for making a decision. This is particularly the case on more contentious issues. Reviews can often get stuck if no one wants to make the final decision. As always, take account of all opinions but try not to let policy get stuck on this. Maybe make a softer policy statement in the interests of getting something published. You might find in 6 months things have changed and a decision can be reflected in a more strongly-worded updated policy.

Policy is Unclear

If people can't understand or interpret your policies, they are unlikely to comply with them. Indeed, policies shouldn't be open to interpretation; they should be clear and concise, with each statement having only one possible meaning. To ensure this is the case, use a style guide and the services of a technical writer or an editor for each policy. Make sure you have a proper final review process in place where your policy is proof-read before being published. This should get rid of any last-minute typos or issues that will prevent comprehension.

5. Reviewing the Information Security Policy

Policies should reflect current needs, but things change over time – the agency may lose or gain functions, restructure itself, adopt new technology or introduce new ways of working. These events may affect the management of information which support business and operations and bring a need to review, and probably update, the policy and procedures underpinning information security.

The policy should be reviewed and, if necessary, amended so that it is kept up to date and continues to meet the agency's needs. Agencies need to decide the frequency of periodic review for themselves. Agencies need to review the policy after major organisational or technological changes. Identification of issues that require attention during monitoring is another trigger.

When reviewing existing policies, a number of factors should be taken into account in addition to those included during the initial development. The experience of working with the existing policy by users, systems administrators, or anyone else who has seen the policy in action is valuable here. These people should be interviewed on how they think the policy worked and what could be changed in the future. They will also provide valuable insights into changes in technology or industry best practices that may need to be reflected by a change in the policy. Any security violations, deviations, and relevant audit information should also be considered when reviewing existing policy. This information will highlight any areas where the policy was difficult to enforce or where frequent deviations from policy were noted. It may be that elements of the policy are infeasible or need to be changed slightly to ensure that extra and unnecessary work on deviations is not created. This must as always be balanced with good security practice. Policy must primarily reflect what is necessary for good security. From a due diligence viewpoint, it is not acceptable to change good policy to inadequate policy, just because there were a number of requests to deviate from that policy by certain groups within the agency.

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email gisu@education.tas.gov.au

Acknowledgements

- Information Standard 18: Information Security – Implementation Guideline, Queensland Government ICT Policy and Coordination Office, Department of Public Works

- Information Security Internal Governance Guideline, Queensland Government ICT Policy and Coordination Office, Department of Public Works
- Information Steering Committee Terms of Reference, Queensland Government ICT Policy and Coordination Office, Department of Public Works
- AS/NZS ISO/IEC 27001:2006 Information technology – Security Techniques – Information security management systems – Requirements
- ISO/IEC27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary
- Information Security Policy Development Guide for Small and Large Companies, SANS Organisation, http://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331?show=information-security-policy-development-guide-large-small-companies-1331&cat=policyissues Viewed on November 2013
- Thanks to Angela Males and the Department of Police and Emergency Management for an example of how to implement an agency wide information security policy framework

Information security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History

Build Status

Version	Date	Author	Reason	Sections
1.0	November 2013	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
		This is the first release of this document.

Issued: November 2013

Ross Latham
State Archivist