
Corporate policy on electronic records

Standards for the management of Government records

Corporate policy on electronic records

© Crown copyright September 2000
Version 1

Public Record Office

Kew,

Richmond,

Surrey

website: *<http://www.pro.gov.uk/recordsmanagement/default.htm>*

Contents

1: Summary	1
2: Introduction	3
Guidance from the PRO	
Why do we need a corporate policy on electronic records?	
Relationship with the 2004 target	
Relationship with Freedom of Information	
Intended audience	
3: Planning the policy	7
Overview	
Methods and mechanisms	
4: What a policy should cover	9
Overview	
Requirements	
Example statement on policy requirements	
Example statement on record requirements	
Example statement on process requirements	
Example statement on transitional requirements	
5: Policy framework	13
Overview	
Example statement on linked policies	
6: Implementing the policy	15
Putting the electronic records policy into practice	
Corporate standards for handling electronic goods	
7: Technical policy	17
Overview	
Methods and mechanisms	
Example statement on technical criteria	
8: Preservation policy	19
Overview	
Methods and mechanisms	
Example statement on changes in infrastructure	

9: Registration policy	21
Overview	
Methods and mechanisms	
Example statement on approach to registration	

10: Access policy	23
Overview	
Methods and mechanisms	
Example statement on access controls	

11: Security policy	25
Overview	
Methods and mechanisms	
Example statement on security controls	

12: Policy audit	27
Overview	
Methods and mechanisms	
Example statement on planned audit	

References	29
-------------------	----

1: Summary

Purpose of the guidance and relationship with the 2004 target and FoI

1.1 This section summarises the contents of this guidance. It is aimed at Departmental Record Officers and other personnel charged with records management responsibilities to meet the corporate policy milestone, which follows:

A corporate policy to be in operation setting out integrated principles for management of electronic records in existing and new systems to guide procedures and user practices.

1.2 The guidance is designed so that a corporate policy for electronic records can be developed in a clearly defined manner, and be put into operation, as a step on the e-records Route Map (see *Reference* section) to achieve the Modernising Government 2004 target.

1.3 It will also assist departments to meet the obligation under the forthcoming Freedom of Information (FoI) legislation to have a policy in operation for records management.

Relationship with departmental e-business strategy

1.4 The corporate policy for electronic records (it will from here on be referred to as the policy) will also complement a department's e-business strategy required by the e-Envoy.

Benefits of the policy

1.5 A corporate policy which sets out the generic principles that should apply to the management of electronic records across the organisation, and which has received formal approval at senior management level, will provide a solid platform for incorporating the general principles of electronic records management into day-to-day operations.

Aims of the policy

1.6 A policy for electronic records should aim to:

- Provide clear guidance on what electronic records are and why they need to be kept.
- Explain how good electronic records management will serve major needs of the department.
- Set out generic principles and policies on specific aspects which then form the basis of implementation.
- Define responsibilities for records throughout the organisation.

Reading guide

1.7 Since this guideline is one piece of a range of guidance, it is recommended that the overall guidance on electronic records be read first as well as the Route Map to put the policy milestone in context with other milestones (see *Reference section for Management , Appraisal and Preservation of Electronic Records Vol. 1: Principles and e-records: Route Map and Milestones to Achieve Electronic Records Management by 2004*).

1.8 It is suggested that the reader then studies this summary to understand the structure and purpose of this document and subsequently goes to section 3 on planning the policy.

Planning the policy

1.9 It is necessary to plan the development and implementation of the policy to gain formal authority, consult many areas of the organisation and produce the policy with an overall implementation plan. Planning the policy is covered in Section 3.

What a policy should cover

1.10 A policy should cover electronic records as a corporate resource (Section 4) as well as covering specific aspects (Sections 7 to 11).

Policy framework

1.11 Section 5 provides advice on relating the policy on electronic records to other policies in the organisation.

Implementing the policy

1.12 Section 6 covers implementation of the policy and how it relates to procedures on electronic records.

Policy review

1.13 Section 12 covers a process to deal with policy changes.

References

1.14 A list of references used, or otherwise useful, is given at the end of this document.

2: Introduction – providing a context

Guidance from the PRO

2.1 The Public Record Office produces guidance covering a wide range of topics to meet the needs for organisations and individuals. The series produced by the Records Management Department at the PRO on the *Management, Appraisal and Preservation of Electronic Records* starting with *Vol. 1: Principles* and *Vol. 2: Procedures*, is now being complemented by detailed guidelines and toolkits. These are intended to provide practical guidance on how to implement these principles and procedures. This guidance is provided as an extension of the existing guideline on policy development for electronic records given in sections 2.21-2.59 of *Management, appraisal and preservation of electronic records: Vol. 1 Principles*. It is intended to facilitate the development of a policy by Departmental Record Officers (DROs) within their own departments and agencies.

Why do we need a corporate policy for electronic records?

2.2 A policy for electronic records management is needed to ensure that:

- the record is present
The organisation has the information that is needed to form a reconstruction of activities or transactions that have taken place.
- the record can be accessed
It is possible to locate and access the information, by use of appropriate software and hardware, and display it in a way consistent with initial use
- the record can be interpreted
It is possible to establish the context of the record: who created the document, during which business process, and how the record is related to other records
- the record can be trusted
The record reliably represents the information that was actually used in or created by the business process, and its integrity and authenticity can be demonstrated
- the record can be maintained through time
These qualities of accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite migration between hardware, digital media, or software formats.

2.3 The first three items are commonly found in a general organisational information policy, aiming to ensure that:

- the right information is captured, stored, retrieved and preserved according to needs
- it is fully exploited to meet current and future needs, and to support change and development
- it is accessible and meaningful, in the right format, to those who need to use it
- and that the appropriate technical, organisational and human resource elements exist to make this possible.

2.4 The remaining items (trustworthiness and permanence) carry special implications for records, and influence the way in which the first three can be implemented. In order to achieve these qualities for electronic records, formal policy statements (together with a commitment to those policies by the organisation) can offer the corporate authority and institutional guidance which records managers require.

Relationship with the 2004 target

2.5 This toolkit is one of a set that offers practical guidance for public record bodies so that they are better placed to meet the 2004 target for electronic records within the overall e-government strategy. This states that:

by 2004 all newly created public records should be electronically stored and retrieved.

2.6 In particular, the guidelines and toolkits seek to support the work needed to meet the milestones in the e-records Route Map (see *Annexes* for reference), which government departments are being asked to achieve en route to the 2004 target. The relevant milestone concerning the policy is:

A corporate policy to be in operation setting out integrated principles for management of electronic records in existing and new systems to guide procedures and user practices.

Relationship with Freedom of Information (FoI)

2.7 The creation of a policy will also assist departments to meet their pending obligations under the proposed FoI legislation. The draft *Lord Chancellor's Code Of Practice On The Management Of Records Under Freedom Of Information version 21a (21 June 2000) section 6* states:

An authority should have in place an overall policy statement, endorsed by top management and made readily available to staff at all levels of the organisation, on how it manages its records, including electronic records.

Intended Audience

2.8 This toolkit is designed to assist Departmental Record Officers and other personnel charged with records management responsibilities to develop the policy.

2.9 There will be other people in the organisation who are required to support the policy once it is up and running. These are covered in section 6. They will need to take this knowledge forward throughout the organisation and use it to inform the organisation's procedures.

2.10 The guidance is intended primarily for those working in public record bodies i.e. central government; the principles as they underpin the e-government strategy, will also be relevant in local government and throughout the public sector.

2.11 Throughout this document the term ‘department’ should be taken to apply to any public sector organisation, including all departments, agencies and other organisations across government. Familiarity with the concepts of records as used in central government is assumed – see *References* section for more information.

3: Planning the policy

Overview

3.1 A corporate policy aims to identify general principles which can be applied to varying situations, taking different operational and technical forms, yet still achieve a common standard across the organisation. A policy should not, though, be pitched so broadly that everyone can agree with it but no-one feels the need to do anything about it - a balance is necessary between these two.

3.2 Without being prescriptive in terms of procedures, an electronic records policy should be formulated to put an emphasis on activities and include basic monitoring mechanisms to see how well it performs. It should change and develop as a result of feedback on implementation and remain consistent with changes in the organisational, legal and technical environment.

3.3 Most important of all, a corporate policy must be agreed to. Writing the words of a policy statement is much less difficult than the process of gaining agreement to them; without this, the policy intentions will be diluted or abandoned and it will be more difficult to retrieve the situation - a policy which is ignored is worse than no policy at all. It is important therefore, that the various stakeholders have an opportunity to contribute to the discussions, that the policy is sponsored by a senior management 'champion' and that once developed the policy is adopted formally and disseminated widely.

3.4 While a policy by itself does not solve all current problems, it provides a framework which can be applied in progressive stages to specific areas of electronic records activity in the department. This framework can guide newly developing information systems and records-creating processes at the same time as incrementally drawing current practice within its umbrella.

Methods and mechanisms

3.5 Individual circumstances for an organisation mean that the approach taken in this guidance is modular. Every module may not apply to every organisation that requires a policy; it may be appropriate for organisations to adapt only a few modules to fit their current policy framework.

3.6 Organisations following these guidelines will be able to define the:

- requirements to be met by the policy concerning the records,
- processes and transitional arrangements to address in moving towards full electronic records management
- positioning of the policy in the policy framework of the organisation,
- implementation of the policy.

3.7 The plan needs to deliver a policy which consists of an overall policy section, a framework section and individual sections on implementation, technical aspects, preservation, registration, access and security. Each of these parts of the policy are covered in sections 4-11 of this document. Realistically, it is expected that a comprehensive understanding of the issues and the requirements involved in electronic records management will only be formed while the policy is in use.

3.8 Once the policy is operational, it should be reviewed on a regular basis to take into account changes in circumstances or to make policy guidelines more explicit where there is any uncertainty about implementation.

3.9 The development of the policy should be approved at each stage. A formal plan for its development should be produced, including the circulation, consultation, approval, issuing, implementation and monitoring activities.

3.10 Development of the policy may be through staged implementation; for example, gradually addressing different parts of the organisation, different business areas or different business processes.

3.11 Developing an active and working policy requires commitment. There is a need to look into the present policy situation and match this to the ideal, trying to base the policy on what can be done within the current framework. A draft policy will be an essential first stage. It will act as a consultative document and can highlight any areas of concern. Eventually the comprehensive, fully operational policy will be put in place.

3.12 The development plan should cover:

- approval mechanisms for the draft policy statements that involves consultation with users and managing body and approval for each stage of the policy development
- development, updating and possible re-issuing of the policy to ensure that it meets the needs of the organisation and relevant strategies across government
- roles and responsibilities for implementing policies and developing associated procedures
- adoption of the policy across the organisation with a phased implementation divided into stages and tested out on a trial basis
- a mechanism for drafting guidance to the organisation for interpretation of the policy. The plan should detail which individuals will be responsible for creating the guidance, at what level these are to be approved and how these fit into a policy.

4: What a policy should cover

Overview

- 4.1 The overall policy should be stated with sections on:
- The purpose of the policy
 - Scope
 - Meaning of records and needs for records in the organisation
 - Requirements for records management
 - Principles
 - Followed by topics as in sections 5-12 in this guidance.

4.2 Strategic planning towards the introduction of electronic records may require transitional objectives as organisations develop their e-business strategies and start to implement new ways of working. An investigation into the current processes for dealing with paper records and their original electronic forms will identify specific requirements that the policy should consider. An example might be: ‘Electronic records will be created by the originating area with a registration number consistent with a corporate fileplan that covers paper and electronic records.’

Requirements

4.3 The following statement and subsequent examples in this guidance describe what each policy section should cover.

Example statement on the scope of the policy

4.4 This policy aims to meet the requirements of good records management to cover all the electronic record collections and planned electronic records of the <<ORGANISATION>>. The policy covers:

- the requirements that must be met for the records themselves to be considered as a proper record of the activity of the organisation
- the requirements for systems and processes that deal with records the quality and reliability which must be maintained to provide a valuable information and knowledge resource for the whole organisation
- its place within the strategic and policy framework of the organisation
- the implementation plan across the organisation
- the use of approved technical solutions
- the resources needed to preserve the record intact
- the policy governing Registration process
- the policy governing access
- the policy governing security
- the policy for reviewing the policy and checking the quality of implementation.

4.5 These will be updated according to a development plan issued within the policy making areas of the <<ORGANISATION>>.

Example statement on records management requirements

4.6 The following example statement covers records management requirements. It should be incorporated into the policy to give the reader a clear idea of the importance of a 'record' in electronic form versus the idea of an electronic document:

Electronic records within the <<ORGANISATION>> are to be clearly identified following a pattern of treatment similar to that previously given to paper records. They must be able to be preserved and stored for the required period within the <<ORGANISATION>>. They will be selected using defined selection criteria and can be transferred to other organisations for future preservation, or destroyed once they are no longer of operational use. In order to ensure that the information constitutes a record the organisation is required and endeavours at all times to ensure that:

- the record is present
The information needed to reconstruct activities and transactions that have taken place is recorded.
- the record can be accessed
It is possible to locate and access the information and present it in a way that is true to the original presentation of the information
- the record can be interpreted
A context for the information can be established showing when, where and who created it, how it was used and how it is related to other information
- the record can be trusted
The information and its representation exactly matches that which was actually created and used, and its integrity and authenticity can be demonstrated beyond reasonable doubt
- the record can be maintained
The record can be deemed to be present and can be accessed, interpreted and trusted for as long as necessary and on transfer to other approved locations, systems and technologies.

4.7 The importance of maintaining a corporate memory of events and activities, means that resources will be needed for the proper management of systems and processes that deal with electronic records and potential electronic records.

Example statement on process requirements

4.8 The following example deals generally with these system and process requirements.

The <<ORGANISATION>> deems that electronic records are an asset that requires careful control and the diligent application of standards to all systems and processes within the organisation. The systems and processes will be required to:

- identify whether they deal with records, electronic records or potential electronic records
- if they do deal with such records, the system or process must maintain them so that the record nature remains intact
- provide information on the records or potential records as required for inclusion as part of a collection in the inventory of record collections
- provide the records for registration, transfer or disposal according to the records management guidance
- keep the records secure and monitor access in accordance with records management guidance
- have regard for legal requirements such as Data Protection, Freedom of Information and copyright legislation.

Example statement on transitional requirements

4.9 Records will have already been created or acquired by a variety of routes within the typical organisation. The electronic creation and processing of information by individuals in the organisation may sometimes mean it is not captured on the record file when it should be. There is a risk of information being lost when the notion of electronic records is adopted but not fully implemented. Any guidance issued to the organisation must be clear about what is covered. The records management requirements given in the earlier example statement must be stressed.

4.10 The aim is to ensure that electronic documents considered to be records should become part of a controlled set of electronic records or as an interim measure should be printed and committed to the paper files.

4.11 However it is necessary to have a statement of intent to achieve 100% of newly created records being stored and retrieved electronically to meet the 2004 target. This 100% target should be broken down into achievable steps expressed as interim percentage targets or as coverage of specified areas of the organisation in the period leading up to 2004.

4.12 While the organisation is moving towards full electronic records management, there is a requirement to clearly distinguish whether the record is electronic or in the paper file. An example of the statement that covers this changeover is as follows.

The <<ORGANISATION>> will monitor electronic records and potential electronic records to ensure that:

- records that should be captured are being processed electronically if they do not appear in the paper record
- there is no unwarranted duplication between the paper and electronic record collections
- there is a distinction made between the electronic documents which are printed, printed records that reside in the paper record systems and other
- original documents that are retained as electronic records (possibly to be passed to an electronic record keeping system)
- an inventory of record collections will be created to ascertain the nature and type of records and potential records within collections. Care must be taken to ensure a good level of control of the record creating systems and that the records nature is preserved appropriately in the transitional period
- the implementation of any Record Management System should clearly show where the record is located and in which form it is held.

5: Policy framework

Overview

5.1 The policy for electronic records may be merged with a general corporate policy for records or kept separate. Either way, it needs to relate to other policies.

Example statement on linked policies

5.2 Maintaining the effectiveness of the policy means the interaction between the electronic records policy and other policies should be stated. This can be accomplished within the policy by a statement similar to the following.

There will be requirements in other policies that electronic records must meet. The following are made explicit by reference:

- following best practice
Electronic records should be managed in accordance with relevant codes of practice for records management – in particular, the forthcoming ISO/CD 18489-1 which provides an overall guide to best practice in records management
- the department's e-business strategy
Electronic records will underpin e-business providing records for business use, corporate knowledge management and evidence-based policy making, evidence for accountability and historical use.
- Freedom of Information
Electronic records will have to adhere to procedures under the forthcoming Freedom of Information legislation and the associated Lord Chancellor's Code of Practice on the Management of Records
- Data Protection
Electronic records will have to adhere to procedures under the Data Protection Act 1998.
- existing records policy
(that is, paper-based policies)
- audit policy
Electronic records will have to meet audit requirements.

6: Implementing the policy

Putting the electronic records policy into practice

6.1 The policy should be communicated from the top of the organisation in a summary form which everyone will read and understand.

6.2 The full policy should be provided to the people who have a part to play in its implementation and further development.

6.3 The formal policy statement should be supported by an electronic records strategy, as a separate follow-on exercise. This will identify a future position which the organisation will aim to reach within a defined time period, appraise the current situation and the issues in achieving this goal, and identify stages which guide action. The strategy will indicate the appropriate timescales within which each identified stage should be achieved, and the means by which the progress of the strategy can be monitored.

6.4 Procedures will need to be developed later, in line with the policy, and should be embedded in the ways people work. They can support the strategy by spelling out the implications of general policy in terms of practice in specific areas of activity, for example:

- codes of practice, standards and statements of best practice
- procedures for electronic records management
- procedures and guidance for users in creating and capturing records
- system design criteria in developing record-keeping systems
- responsibilities in managing records for specific organisational roles.

Corporate standards for handling electronic records

6.5 Effective records management is one element within corporate information management. It should be co-ordinated with, and contribute to the development of, the corporate information strategy. The adoption of corporate procedures and standards is essential to ensure that effective records management is consistently provided for the organisation, in a systematic and sustainable manner.

6.6 Everyone within an organisation is involved in electronic record-keeping and is responsible within their own sphere of action for ensuring that evidence of business activity is created and recorded. Appropriate implementation measures might take the form of a code of practice, backed up by a programme of training and user workshops.

6.7 The four main groups who have some form of responsibility for the implementation of policy on electronic records are:

- records managers and information managers
- information systems and information technology managers
- business managers and process owners
- end users.

6.8 More detail on the above is given in the in sections 2.54-2.57 of *Management, appraisal and preservation of electronic records: Vol. 1 Principles*.

6.9 In addition further assistance with procedures will be provided in forthcoming guidelines (listed in the *e-records Route Map*).

7: Technical policy

Overview

7.1 The inclusion of a technical policy establishes the criteria to be applied to the technologies that process electronic records. The use of new types of technologies can also be judged against the technical policy. These new technologies can then be considered to be compliant to the policy and therefore acceptable for electronic records, or not to be compliant and only allow for working ephemeral documents.

Methods and mechanisms

7.2 Cross-government strategies and individual organisations' IT strategies will set requirements for the IT systems in more general terms. It is essential to appreciate how they affect electronic records and records management (see *References* section). A summary of the technical properties of currently employed technologies should be drawn up and some distinctions may be made between structured technologies, such as databases, and unstructured technologies, such as office word processes, which are often customised by users. Highly structured records are easier to manage than documents that may have been uniquely structured by users.

Example statement on approach to registration

7.3 Since not all technologies will have been designed with electronic records management in mind, the use of technology to process electronic records must be subject to certain design criteria (see *Management, approval and preservation of electronic records Vol2: Procedures* for more information on this topic). These criteria may change and adapt to new technologies as they appear. However, they should inform the take up of controlled technologies. The following statement covers the use of technologies and how they can be judged against design criteria.

The <<ORGANISATION>> applies technical criteria to the technologies that process electronic records. This ensures that:

- it is technically possible for the electronic records to meet record requirements starting from when they are created and for as long as they are needed
- systems will be selected on the basis of how well they will cope with electronic records, to prevent any loss of the record because of incompatibility or insufficient safeguards being used
- records management systems adhere to the minimum functional requirements as stated in the PRO publication *Functional Requirements for Electronic Records Management Systems*.
- the systems designed for records management are capable of and useful for record keeping activities
- metadata is captured and can be used for referencing the information by using defined terms that are user-friendly and accurate.

8: Preservation policy

Overview

8.1 A preservation policy helps to ensure that electronic records are visibly present and maintained in an authentic state. The technology that serves to process the electronic record will change over time, but the preservation policy should seek to minimise the risks associated with any technological changes and ensure that the records remain intact. The preservation policy should also seek to allow for any non-technical changes. For example, electronic records should always have an associated context and remain comprehensible as the organisational structure changes.

Methods and mechanisms

8.2 A list of generic risks inherent in systems that process electronic records can help to formulate a more comprehensive preservation policy. The preservation policy can refer to the use of an inventory of record collections that will indicate which systems are being used to store and manage the electronic records. Knowledge of how systems are administered could be tied into the preservation policy so that practical and resource efficient safeguards are put into place. In addition, the process for gathering information about the changes in staff roles and administrative set-up can be brought into line with the policy.

Example statement on access controls

8.3 Once an electronic record is formed, the record and its use will be subject to the preservation policy. The record should not alter because the holding system changes. Any activity that generates the record will also have to place it in the relevant context (in other words, the context needs preserving as much as the original record). The preservation of the record's form, information, metadata and contextual meaning helps to ensure that the context is not lost. The following statement suggests an approach to address changing infrastructure.

The <<ORGANISATION>> seeks to preserve electronic records during any change in the infrastructure so that they can still satisfy the original policy requirements. Preservation needs must be satisfied when there are changes in:

- the technology that processes the electronic records how this affects the way records are processed throughout the records' existence
- organisational structures and how these are interpreted and give the records context
- the definition of terms used in the metadata and within the records themselves
- the classification of the electronic records including how the records are grouped and described so that they can be presented in a way consistent with the original understanding of the subject when the record was created.

9: Registration policy

Overview

9.1 A registration policy helps the organisation to set minimum conditions for the registration of electronic records, so ensuring a link between the electronic record and its administrative roots.

9.2 The registration policy should be broad enough to standardise registration systems, so that the electronic records are well organised and can be discovered by a third party. It should not be so restrictive that the records are arranged or labelled in a cumbersome way and slow down operational efficiency. The registration policy may cover a number of systems in either paper or electronic form but it should help to establish a uniform method across the organisation, possibly within an integrated solution.

Methods and mechanisms

9.3 A study of the generic process of registering paper files may identify what is expected from the registration procedures. For example, paper files should be classified into series and sub-series lists so that cataloguing can be easily achieved. Apart from the other system-related conditions that may be dealt with by a technical policy, the registration policy might include statements that help formulate cross-checks on the registration of records. A series could be cross-referenced to business functions and workflows.

Example statement on approach to registration

9.4 The registration policy has to be specifically tailored to the needs of the organisation. Registration can be done at many levels and within a range of systems. Responsibilities can be allocated to various personnel and parts of the organisation to ensure that the registration makes sense of the records. There should be a common approach, one that can be followed in an audit, and that also takes into account the variety of records that may arise. An example of the approach is shown below, which should be adapted to the organisation's specific needs.

The registration of electronic records will follow best practice in records management and allow for the users of the records to identify and track particular records and record collections.

The approach the <<ORGANISATION>>has to registration involves:

- classifying of the records into series that have meaningful titles and a consistent reference code
- setting a responsibility on individuals forming record items to allocate them to a series and if necessary a sub-series or sub-sub-series
- having sequences of reference numbers that can cover series with both electronic and paper records
- checking that the correct records have been allocated to the sequence and that meaningful titles are used
- auditing lists of the references used so that the registration system makes sense and records can be found in appropriate search sequences.

10: Access policy

Overview

10.1 An access policy helps to control the movement of information in and out of the records management systems, allowing the records to be created or viewed by different categories of users.

Methods and mechanisms

10.2 The access policy establishes how access to the electronic record series is to be assessed and where this responsibility should lie. An access policy may also seek to set limits on access depending on the type and origin of the record as well as its content nature.

10.3 An awareness is needed of constraints that affect the types of information processed. Is the record subject to copyright restrictions, data protection, Freedom of Information, confidentiality or any other specific laws or considerations?

10.4 The access policy can make use of an inventory of record collections that will indicate how the electronic records are processed and what conditions should be attached to any process. An outline of the administrative framework of the organisation could be linked to the access policy so that responsibilities are made explicit. Alternatively, general titles or groups may be used which are then linked to the administrative framework by working procedures.

Example statement on access controls

10.5 The presence of an access policy determines decisions about the accessibility of the electronic records. There will be both external and internal needs to cater for. Ideally, there should be a rigorous code that is enforceable by the technology or through the registration process and a control on the physical location of the records.

10.6 The following example statement uses the phrase 'roles or bodies within the organisation'; this should be replaced by the specific names involved.

The <<ORGANISATION>> will use access controls to allow the records to be viewed by all relevant parties, and offer a mechanism for opening up some of the information for use outside this group.

The actual controls will depend on many factors but the general principles can be summarised as:

- electronic records will be made available for continuity of actions. The creators and managing individuals or groups should have access to relevant information
- roles or bodies within the organisation which have been identified as being able to make an accurate judgement will decide on the sensitivity of the record. This judgement may be on a whole series or simply cover individual items. It will identify any restrictions on the records and it will highlight any groups or individuals within the organisation who should have access
- any judgements, including any background reasons for withholding or masking information within the record or record series, are to be recorded. The resulting record will be kept for at least as long as the records in question; however it may not have the same access status as the main record
- the organisation will not seek to put blanket restrictions on a record series if only some of the individual records are judged sensitive
- electronic records are subject to the Public Records Act 1958 and the organisation will ensure that they are treated accordingly. Access will be needed for appraisal decisions to be implemented. The nature of the access will be defined for records judged to be of a sensitive nature
- information taken from the records or record metadata may be subject to legislation requiring it to be either withheld or made more widely available outside normal business needs (or even outside the organisation itself). For example there may be a need for compliance with data protection or Freedom of Information legislation
- all records are part of the corporate memory. Unless restricted, due to legislation or as a result of a judgement, they will be made readily available within the organisation. This may be subject to volume restrictions because of technical limitations or copyright reasons
- any access arrangements will be made for a specified duration and these will be reviewed according to a schedule identified during appraisal.

11: Security policy

Overview

11.1 A security policy helps to build confidence in the management of records. It should seek to protect the record management infrastructure as well as safeguard individual records from interference and misrepresentation. The security policy might identify some types of restriction on access. However, if these are placed within an access policy, they can be made more coherent with the other issues relating to access.

Methods and mechanisms

11.2 A summary analysis of staffing and resources available for creation and management of records should highlight any priorities and help the security policy to concentrate efforts on easily implemented security measures.

11.3 An investigation into a specialised audit or the implementation of systems for checking processes such as access and transfers may offer additional levels of protection and help to guide policy decisions.

11.4 An interrogation of the individual stages of the record keeping may identify areas of concern. A list of questions could be formulated to test how secure the stages are and grade according to their security risk status. A risk assessment, including their criticality to the process, would then indicate whether the security risks need to be addressed quickly, by enforcement of the policy within normal operating environment, or whether they can become part of the procedures in due course.

Example statement on security controls

11.5 Risks can be greatly reduced with security controls. They may deal with explicit risks or in general allow for procedures to govern risk as they are identified. The following example statement about security controls highlights the general areas of risk. It should be modified to take into account specific issues within the organisation.

The <<ORGANISATION>> takes all reasonable steps to ensure that the electronic records and processes dealing with them are secure. Once recorded and registered in the system, they will be safe from alteration, misinterpretation or loss.

The steps include:

- informing staff and complying with records management best practice
- using a corporate policy and organisational procedures, where they exist, and helping to determine new policy and procedures where they do not
- training staff to use the records management systems for an accurate representation of the records using only relevant metadata, thereby ensuring consistency in record registration and metadata without loss of context and control
- auditing the systems to trace any deviation from procedure
- offering solutions to rectify mistakes or altering the procedures to accommodate better ways of working
- setting up business continuity plans to ensure a constant service is maintained in spite of any technical or strategic hitches that may occur
- enforcing access restrictions with user IDs and passwords, setting user lockouts
- maintaining disaster recovery plans that include replicating electronic records on a physically secure back-up and safeguarding the information from technical failures.
- implementing strict back-up cycles with updates for new records and metadata, ensuring that any destroyed or transferred records are also promptly physically cleaned from the back-ups
- labelling the replicated records as a replica set and making sure these cannot be used as the master set, unless the original has been destroyed accidentally or following a disaster

12: Policy review

Outline

12.1 Review should answer the questions:

- is everyone, who should be, aware of the existence of the policy and its contents?
- is everyone, who should do so, following the policy correctly?
- if not, what remedial action can be taken?

12.2 A policy review can be used to increase the effectiveness of the operational policy by establishing how it is interpreted within the organisation and suggesting changes where there is uncertainty. It will highlight the dependencies between the activities, procedures and areas of policy, helping to ensure that these all work together in a seamless manner.

12.3 A policy may have been implemented for operational reasons in one part of the organisation in a way that does not suit the requirements of some other areas. The policy review could help to identify common policy combined with a clearer distinction between policy and procedures. Specific requirements are thus addressed with localised procedures.

12.4 A policy review will indicate if the policy needs to be amended, as changes occur in the organisational structure or workflow.

Methods and mechanisms

12.5 A policy review should be planned review should identify actions and responsibilities. The review may be conducted on a routine basis, in response to internal or external stimuli, or both.

12.6 An awareness of any audit trails at the activity and procedural level will be useful when reviewing. They may identify where effort should be maximised and what type of procedure or policy is needed. For example, if transfers being made in various formats are a cause of confusion and the current procedures do not specify a format, then a policy should be written to state that transfers are to be made according to set standards and indicate where these are to be found.

12.7 A complete audit may be accomplished only over a prolonged period of time with much iteration. Thought should be given to providing the most efficient way of reviewing the policy for an organisation. For example, is it best accomplished unit by unit or by following the workflow patterns? If a planned review identifies that changes are needed in the policy, then their implementation including approval mechanisms, impact on the policy framework and adherence to the other policy sections should be considered.

**Example statement on
planned review**

12.8 The policy will affect the records management procedures that are already in place and the impact of the development plan will mean that new procedures and/or guidance may have to be introduced. This could mean that the policy is not uniformly interpreted within different parts of the organisation or that certain parts of the organisation may require substantial help in achieving the intended aims of the policy.

12.9 Operational testing of the policy and a system for developing of common guidance or procedures is essential. The planned review of the policy and procedures could be important in helping the policy become reality. The following example statement incorporates testing and endorsement as part of the policy itself. Alternatively it may be placed in a higher level policy and a simple statement in the policy may be used to refer to it.

The <<ORGANISATION>> will endeavour to follow the policy within all relevant procedures and guidance used for operational activities. Interpretation of the policy will be monitored and there will be a regular planned audit to assess how the policy is being put into practice.

The audit will seek to:

- identify areas of operation that are covered or not covered by the policy and to identify which procedures and/or guidance should adhere to the policy
- follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of electronic records and use a subsidiary development plan if there are major changes to be made
- set requirements by implementing new procedures, including obtaining feedback where the procedures do not match the desired activity
- highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures such as security and access.

References

Management, Appraisal and Preservation of Electronic Records

Vol 1: Principles *

Vol 2: Procedures *

PRO

2nd Edition, Crown Copyright 1999

Guidance for an Inventory of Record Collections

A toolkit *

PRO

Crown Copyright 2000

Data Protection Act 1998

A Guide for Records Managers and Archivists

PRO/Public Record Office Northern Ireland/The National Archives of Scotland

Published in association with the Office of the Data Protection Commissioner, Crown Copyright 2000

*The Draft Lord Chancellor's Code of Practice on Management of Records under the Freedom of Information**

Version 21a, 21 June 2000

Information Age Government Framework for ERM and e-records Route Map

The Modernising Government milestones are presented in the Electronic Records Management framework and the e-records: Route Map and Milestones to Achieve Electronic Records Management by 2004* published as supporting guidelines on the Information Age Government Champions website:

<http://www.iagchampions.gov.uk/Guidelines.htm>

The Modernising Government target states:

'It is our aim that by 2004 all newly created public records will be electronically stored and retrieved.'

This is presented in the *Modernising Government White Paper* available from:

<http://www.citu.gov.uk/moderngov/whitepaper/4310.htm>

Items marked * are available in the Records Management area of the Public Record Office website:

<http://www.pro.gov.uk/recordsmanagement/default.htm>