

## **Preamble**

Records and recordkeeping are inextricably linked with any organized activity. It is only through the information an organization records in the normal course of business that it can know what it has done and effectively plan what it will do in the future. As a key resource in the operation of any organization, records must be created, organized, secured, maintained, and used in a way that effectively supports the activity of that organization, including:

- Facilitating and sustaining day-to-day operations
  - Supporting predictive activities such as budgeting and planning
  - Assisting in answering questions about past decisions and activities
  - Demonstrating and documenting compliance with applicable laws, regulations, and standards
- 
- **Principle of Accountability**  
An organization shall assign a senior executive who will oversee a recordkeeping program and delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure program auditability.
  - **Principle of Integrity**  
A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.
  - **Principle of Protection**  
A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.
  - **Principle of Compliance**  
The recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies.
  - **Principle of Availability**  
An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.
  - **Principle of Retention**  
An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.
  - **Principle of Disposition**  
An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.
  - **Principle of Transparency**  
The processes and activities of an organization's recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.

### **Preamble**

Records and recordkeeping are inextricably linked with any organized activity. It is only through the information an organization records in the normal course of business that it can know what it has done and effectively plan what it will do in the future. As a key resource in the operation of any organization, records must be created, organized, secured, maintained, and used in a way that effectively supports the activity of that organization, including:

- Facilitating and sustaining day-to-day operations
- Supporting predictive activities such as budgeting and planning
- Assisting in answering questions about past decisions and activities
- Demonstrating and documenting compliance with applicable laws, regulations, and standards

These needs can be fulfilled only if recordkeeping is an objective activity, fully insulated from individual and organizational influence or bias. To achieve this transparency, organizations must adhere to objective records and information management standards and principles, regardless of the type of organization, type of activity, or the type, format, or media of the records themselves. Without adherence to these standards and principles, organizations will have poorly run operations, legal compliance failures, and – potentially – a mask for improper or illegal activities.

The principles of recordkeeping have been well developed by those who are fully involved in records and information management. They form the basis upon which every effective records program is built and are the yardstick by which any recordkeeping program is measured. Regardless of whether an organization or its personnel are aware of them, they form the basis upon which that organization's recordkeeping will one day be judged.

It is in the general interest of all organizations, and of society itself, to be fully aware of these principles and to manage records and information assets in accordance with them. ARMA International published these eight Generally Accepted Recordkeeping Principles<sup>SM</sup> to foster general awareness of recordkeeping standards and principles and to assist organizations in developing records systems that comply with them.

These principles are comprehensive in scope, but general in nature. They are not addressed to a specific situation, industry, country, or organization, nor are they intended to set forth a legal rule for compliance that must be strictly adhered to by every organization in every circumstance. They are intended to set forth the characteristics of an effective recordkeeping program, while allowing flexibility based upon the unique circumstances of an organization's size, sophistication, legal environment, or resources. The objectivity of the principles, combined with a reasonable approach to applying them, will yield sound results for any organization: a responsive, effective, and legally compliant recordkeeping system.

### **Principle of Accountability**

**An organization shall assign a senior executive who will oversee a recordkeeping program and delegate responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure auditability.**

- The senior executive in charge should establish a method to design and implement a structure to support the recordkeeping program.
- Governance structure should be established for program development and implementation.
- Necessary components include an accountable person and a developed program.
- A recordkeeping program should have documented and approved policies and procedures to guide its implementation.
- Auditability enables the program to validate its mission and be updated as appropriate.

A basic premise to sound recordkeeping is that within each organization, someone is designated as responsible for the overall program. This does not have to be a full-time responsibility, but it does need to be formally designated to someone in a senior-level position who has access to other senior executives and can ensure program implementation across the organization. The accountable senior executive will oversee the overall recordkeeping program, although this executive often will assign or designate other personnel to roles and tasks involved in different parts of the recordkeeping program.

A major responsibility for this executive is program development. As an on-going program, recordkeeping requires the program to be monitored for compliance and to identify any areas requiring improvement. The matters identified during the monitoring lead to program improvements, which the senior executive will oversee at the appropriate level.

Governance should be established through the organization, assigning defined roles and responsibilities to different staff so it is clear where responsibilities reside and how the chain of command works to build, implement, and upgrade the recordkeeping program. For example, sub-committees can be designated to help build policies or to define and implement technology.

For staff to know how to implement the recordkeeping program, it is essential to have program policies and procedures that are documented, formally approved, and communicated to personnel. Updates to the policy and procedures should be available to staff, as should recordkeeping training. All of this is designed to further standardize the program across the organization. This standardization enhances staff's efforts to effectively implement the recordkeeping program.

*Auditability* is the process designed to prove the program is accomplishing its goals, while seeking areas for improvement to further protect the organization and its records.

- Staff should be able to demonstrate program awareness.
- Records should be retained for the right amount of time and disposed of when no longer required.
- Policies should be kept up-to-date and cover all records media.
- Auditing should verify the status of complying with these standards.

An organization's recordkeeping audits should be reported to the board of directors (or its audit committee) to show program adherence in accordance with documented policies and procedures, requirements (for retention, privacy, access to records, and access controls, for example), and the organization's goals for its recordkeeping program.

### **Principle of Integrity**

**A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.**

*Integrity* of a record is directly related to the ability to prove that a record is authentic and unaltered. *Authenticity* requires proof that a document comes from the person, organization, or other legal entity claiming to be its author or authorizing authority.

An organization's executives are ultimately responsible for business records, as they are strategic and operational assets. Proper corporate governance and integrity of the information are important, and it is necessary to maintain the authenticity of records in all media over time. Investors and government regulators alike should expect the integrity of an organization's records and information.

Integrity of records in a recordkeeping environment should include the following:

- Correctness of and adherence to the policies and procedures of the organization
- Reliability of the information management training and direction given to the employees who interact with all systems
- Reliability of the records created
- An acceptable audit trail
- Reliability of the systems that control the recordkeeping including hardware, network infrastructure, and software

#### ***Correctness of and adherence to the policies and procedures of the corporation***

To defend corporate governance and achieve legal and regulatory compliance, organizations must have implemented formal recordkeeping policies and procedures that have been approved by senior management. If formal support has not been obtained, records may be at risk of not being accepted in evidentiary value.

#### ***Reliability of the information management training***

All employees are responsible to comply with the records management program and should be trained on the meaning, importance, and usage of the corporate policies and procedures.

#### ***Reliability of the records created***

To ensure records are created, used, and managed in the usual and ordinary course of business, organizations must have consistent recordkeeping practices throughout the records life cycle.

#### ***An acceptable audit trail***

Audit trails are essential in proving reliability of the recordkeeping actions of the organization. Acceptable audit and quality assurance processes should be in place.

#### ***Reliability of the system***

The recordkeeping system must be reliable to prove reliability and integrity of the records. A record is only as reliable as the system in which it is maintained.

### **Principle of Protection**

**A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.**

Information generated by an organization in the course of business requires various degrees of protection. Such protection is mandated by laws, regulations, or corporate governance, and it is necessary to ensure that information critical to an organization's continued operation during or after a crisis is available. A recordkeeping program must ensure that appropriate protection controls are applied to information from the moment it is created to the moment it undergoes final disposition. Therefore, every system that generates, stores, and uses information should be examined with the protection principle in mind to ensure that appropriate controls are applied to such systems.

Information protection takes multiple forms. First, each system utilized must have an appropriate security structure so only personnel with the appropriate level of security or clearance can gain access to the information. This includes electronic systems as well as physical systems, using such measures as key card access restrictions and locked cabinets. This also requires that as personnel change jobs, their access controls are changed appropriately and immediately.

Second, this requires protecting information from "leaking" outside the organization. Again, this may take various forms – from preventing the physical files from leaving the premises by various mechanical and electronic means to ensuring that electronic information cannot be e-mailed, downloaded, or otherwise proliferated by people with legitimate access to the system. Sometimes, this information should not even be sent by e-mail – even among parties who have access to it – because such an exchange can jeopardize its security. An organization must also safeguard its sensitive records from becoming available on social networking sites and chat rooms by employees who may either inadvertently or maliciously post it there. It is prudent to have such safeguards clearly defined in organizational policy and, if necessary, to monitor sites for any postings that may violate this rule.

Where appropriate, controls and procedures for declassification of confidential and privileged information should be clearly defined and understood. There may be instances, however, when it may be necessary to allow security clearance exceptions. For example, outside counsel engaged to assist with a litigation action may need to access records that they otherwise would not be cleared to access.

Security and confidentiality must be integral parts of the final disposition processing of the information. Whether the final disposition is an accession to an archive, transfer to another organization, or preservation for permanent storage or destruction, the procedures must consider the principle of protection in defining the process. For example, confidential employee paper files should be handled for disposition only by employees with appropriate clearance and must be shredded or otherwise destroyed in an unrecoverable manner. Classified government records must retain their classification for the appropriate number of years even if they are transferred to an archive.

Finally, an organization's audit program must have a clear process to ascertain whether sensitive information is being handled in accordance with the outlined policies in the principle of protection.

### **Principle of Compliance**

**The recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies.**

It is the duty of every organization to comply with applicable laws, including those for maintaining records. An organization's credibility and legal standing rest upon its ability to demonstrate that it conducts its activities in a lawful manner. The absence or poor quality of the records required to demonstrate this damages an organization's credibility and may impair its standing in legal matters or jeopardize its right to conduct business.

The duty of compliance affects a recordkeeping system in two ways:

1. The recordkeeping system must contain information showing that the organization's activities are conducted in a lawful manner.
2. The recordkeeping system is itself subject to legal requirements such as requirements to maintain tax or other records.

It follows from this that every organization must:

- Know what information must be entered into its records to demonstrate that its activities are being conducted in a lawful manner
- Enter that information into its records in the manner prescribed by law
- Maintain its records in the manner and for the time prescribed by law

An organization that is subject to codes of conduct, ethics rules, or other authorities is subject to a duty to comply with them also. To the extent that recordkeeping is required to demonstrate compliance with the code or rules, or the organization's records system is itself subject to the code or rules, the organization's records must be maintained in accordance with them.

A policy is an internal rule of conduct for the organization and the organization's own statements of what it deems to be correct conduct. By its nature, a policy imposes a duty of compliance upon the organization and its personnel. To comply with laws and other authorities, an organization must adopt and enforce suitable policies to direct and control its recordkeeping.

The precise manner and duties of compliance will vary from organization to organization. Some organizations may be subject to multiple laws and legal doctrines, as well as codes of ethics and other authorities. This may, in turn, require the organization to adopt and enforce multiple and stringent policies for recordkeeping. An organization that is subject to fewer regulations may need fewer recordkeeping policies to maintain compliance. Every organization, however, should draft and enforce its policies and conduct its activities in a manner reasonably calculated to ensure compliance with the totality of authorities applicable to it.

### **Principle of Availability**

**An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.**

Successful and responsible organizations must have the ability to identify, locate, and retrieve the records and related information required to support its ongoing business activities. These records are used by:

- Individuals and groups to reference, share, and support their work
- Legal and compliance for discovery and regulatory review purposes
- Numerous corporate functions to validate management decisions and account for the resources of the organization.

Having the right information available at the right time depends upon an organization's ability to nimbly search through enormous volumes of information.

As more routine business transactions are being conducted exclusively in electronic environments like e-mail, shared local area network drives, collaboration spaces, and websites, this is becoming increasingly difficult to sustain. These electronic environments offer a high degree of individual flexibility in how employees organize the materials they collect on a daily basis. However, this same flexibility results in expensive, time-consuming, and labor-intensive difficulties when specific pieces of electronic information are needed for business or regulatory purposes, months and years after they were originally created. These difficulties are further complicated if the records required are those of employees who have left the organization or of vendors who previously provided records custody for the organization.

Pinpointing complete and accurate information depends on 1) having an efficient and intuitive set of methods and tools to organize the records of the organization and 2) providing employees and agents with sufficient training to utilize these tools successfully. Information must be described during the capture, maintenance, and storage processes in such a way as to make retrieval effective and efficient. A routine approach to capturing descriptive information about the records (known as "metadata") must be documented and utilized in all records systems.

An added complication with electronic information is that even when the media on which it is recorded is available, its accessibility on that media can be uncertain due to its inherent fragility and impermanence. Electronic information needs to be routinely backed up to ensure that it can be restored if there is a disaster, a system malfunctions, or the data becomes corrupted. It also needs to be constantly migrated to currently supported hardware and software to sustain its ongoing accessibility.

To effectively manage the availability of its information assets at a reasonable cost, an organization should in the normal course of business regularly remove obsolete or redundant records and related information from its information systems. This will not only make those remaining records, which have ongoing value to the organization, more identifiable and accessible, but it will also enhance system performance and reduce the maintenance costs of storage, back up, and migration. However, removing unneeded information should occur in adherence with the organization's records retention policies, which should also provide for suspending disposition in the event of pending or ongoing litigation or audit.

An organization's personnel are more likely to retrieve and use information for better decision making and more effective work if it has well-designed storage processes and access to understandable, retrievable, relevant, and consistent information. With properly structured information, personal productivity is improved, storage costs are minimized, and the reliability and speed of retrieval are optimized. Further, complete and accessible records in a well-managed environment minimize inconsistent and erroneous



interpretation of the facts, simplify legal processes and regulatory investigations, and protect valuable information from being lost, corrupted, or stolen.



### **Principle of Retention**

**An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.**

Business and government create enormous quantities of records each business day. To control the growth of these records, an organization needs a program to help maintain and destroy records that are no longer needed. Records retention programs specify the length of time business records must be retained. The retention program is based on the concept that information has a *life cycle*, which is the time period from the creation of a record to its final disposition.

Records document an organization's business operations and are essential to effectively managing that business. The ability to properly and consistently retain records is especially important today, as most records being created and stored are in electronic form.

Organizations make retention decisions based on the content and purpose of records. Retention periods are determined by following these requirements:

- **Legal and regulatory** – Federal, state, local, and even international laws mandate the retention of records and information for a specific period of time. To comply with these extensive laws and regulations, an organization must conduct legal research in consultation with legal counsel to determine all records retention requirements. Laws and regulations establish the minimum retention period for those records to which they pertain. Failure to comply with laws and regulations may result in costly penalties and loss of legal rights.
- **Fiscal** – Records that have financial or tax value must be retained to ensure the timely payment of obligations and the proper receipt of receivables, as well as to support the organization's financial audits and tax returns. Legal research and consultation with legal counsel must be completed to satisfy fiscal retention requirements.
- **Operational** – Once legal, regulatory, and fiscal requirements have been established, an organization must determine how long records are needed to satisfy its business needs. This is usually determined by interviewing the person(s) most knowledgeable about the operational value of each record type.
- **Historical** – Records that depict the history of an organization should be preserved for the life of that organization. Examples of historical records include articles of incorporation, bylaws, charters, and board of directors' minutes. Historical records normally constitute a very small percentage of an organization's total records volume.

Once its records retention requirements are determined, an organization must conduct a risk assessment to determine the appropriate retention period for each type of record. Retention decision makers must be aware that the presence or absence of records can be either helpful or harmful to the organization. Therefore, to minimize risks and costs associated with records retention, it is essential to immediately dispose of records after their retention period expires.



**Principle of Disposition**

**An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.**

At the completion of the retention period for an organization's records, the records must be designated for disposition. In many cases, the disposition for records will be destruction. In other cases, the records may be returned to clients, transferred to another organization in connection with a divestiture, or transferred for ongoing preservation to an historical archives, library, or museum. In all instances, the organization must make a reasonable effort to ensure that all versions and copies of the records are included in the disposition. The organization must also document its disposition process.

If records are converted or migrated to new media, disposition of the previous media may also be warranted.

Disposition of relevant records must be suspended in the event of pending or ongoing litigation or audit. The organization should designate records that are to be held pending resolution of the litigation or audit and notify all affected personnel when the hold is issued and when the hold is released.

Destruction of records must be performed in a secure manner, ensuring that records to be destroyed are transported securely and destroyed completely. The organization may choose to utilize "green" methods of destruction, but destruction must always be performed in a manner that renders the records completely and irreversibly destroyed.

The transfer of records to the custody of a historical archives, library, or museum should be documented as part of the organization's records retention policy. In general, disposition of records in this manner should be governed by appraisal of the records by a qualified professional. The appraisal should be based upon the historical or intrinsic value of the records. In some instances, the organization's records retention policy will designate which records are to be dispositioned in this manner.

### **Principle of Transparency**

**The processes and activities of an organization's recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.**

Many parties have a legitimate interest in understanding the processes that govern the management of a recordkeeping program and the activities undertaken within it. In addition to the organization itself and its personnel, those parties include but are not limited to government authorities, auditors and investigators, litigants, and, for some organizations, the general public.

It is in the best interest of every organization, and of society in general, that all parties clearly understand:

- The organization conducts its activities in a lawful and appropriate manner.
- The recordkeeping system accurately and completely records the activities of the organization.
- The recordkeeping system is itself structured in a lawful and appropriate manner.
- Activities conducted to implement the recordkeeping program are conducted in a lawful and appropriate manner.

The clearest and most durable evidence of these things are records. In the case of a recordkeeping program, those records include recordkeeping policies and procedures and transactional records of the activities undertaken during the course of the recordkeeping program. To ensure that interested parties will have confidence in them, records documenting the recordkeeping program must themselves adhere to the fundamentals of records management. They should:

- Document the principles and processes that govern the program
- Accurately and completely record the activities undertaken to implement the program
- Be written or recorded in a manner that clearly sets forth the information recorded
- Be readily available to legitimately interested parties

The information recorded in these records and the extent to which they are available to interested parties will vary depending upon the circumstances of the organization.

An organization that is subject to open records laws may need to make all records available to any person upon request. Other organizations may have a legitimate need to protect confidential or proprietary information, and they may therefore reasonably put in place procedures designed to control access to information. Complex and highly regulated recordkeeping systems may require extensive records documenting them. Simple systems may require only a few. In each case, however, the rationales and outcomes should be clear to legitimately interested parties.

Every organization must therefore create and manage the records documenting its recordkeeping program to ensure that the structure, processes, and activities of the program are apparent and understandable to legitimately interested parties and that the records documenting the program and its activities are reasonably available to them.