

## **FORMULATING A RECORDS MANAGEMENT POLICIES FOR YOUR ORGANISATION**

The records generated by organisations are a vital source of information to the public, business partners, vendors and clients. Organisations spend a lot of money to create, transmit, and store information; yet insufficient attention is paid to the effective management of these records. Managing the accumulation of records requires a records management program to provide systematic control of all records, regardless of storage medium, from creation, capture or receipt until their ultimate disposition.

A successful program requires policies and procedures that administer the effective control and management of records and information.

### **Policies and Procedures Creation**

There should be written policies and procedures for the management of all organisation's physical records, whether paper, photographic, micrographic, drawings, maps or electronic records. The only way to ensure compliance and consistencies in any organisation's records management program is through written policies and procedures.

The organisation's record management policies and procedures should be based on applicable laws. Organisations should also incorporate its general records management policies into the organisation's policy and procedure manuals distributed to its members of staff.

Some of the issues a basic records management policies should address are as follows:

- Creation, ownership, control, retrieval and filing of records;
- External access to organisation's records;
- Storage and destruction of temporary records in whatever formats;
- Preservation of permanent records in whatever formats;
- Creation and implementation of a disaster recovery plan.

### **Creation, ownership, control, retrieval and filing of records**

The organisation's records management policies should require all employees to create, receive and maintain records that document the business transactions of their businesses. The policies should require that employees create records that are complete, authentic, reliable, usable and provide full and detailed information regarding the activities carried out. The policies should also address the fact that all records created or received in the course of work are records of the state and, as such, must not be disposed of or removed without proper authorization.

Because the integrity of the organisation's records, it must ensured at all times the establishment of filing guidelines that outline the following issues:

- Creation of files and filing systems;
- Utilization of file naming conventions for files;
- Assignment of records management responsibility to employees;
- Reference use of files;
- Returning files to appropriate storage locations after use.

- 

### **External access to organisation's records;**

There should be need for the organisations to formulating an access policy. The policy should cover such issues as:

- Charges associated with providing copies
- Amount of information to be provided and the associated costs
- Hours when records may be accessed;
- Access to fragile records;
- Access to electronic records.

### **Storage and Destruction of Temporary Records in All Formats**

Each record has a retention period as specified in the organisation's document retention policy. The organisation's procedures should ensure that the records are retained for as long as legally required, at which time the records become eligible for final disposition. Employees should be made aware of the retention period, as listed in organisation retention policy.

Some records may become too voluminous for the employee to maintain in organisation office space or computers until the records' retention period has expired. These records should be stored in a location designated by the organisation. The organisation should create procedures that cover the following areas:

- Storage of records;
- Retrieval of records;
- Frequency of destructions;
- Obtaining authorization for destructions from records officers;
- Method of destruction of all record formats (state government policy recommends that paper records be disposed of through recycling);
- Suspension of destruction procedures during audit or litigation;
- Documentation of destructions.

### **Preservation of permanent records in whatever formats;**

Records with a retention period of "Permanent Record" are not to be destroyed. The organisation's procedures for storage of permanent records should ensure that such records are maintained under proper inventory control and in an environment that will ensure their physical order and preservation. Care should be taken in the choice of storage areas for permanent records by considering preservation, safety and access. Organisation storage policies should cover the following:

- Acceptable storage areas;
- Storage of records off the floor and away from pipes and windows;
- Use of smoke detectors, fire alarms, and sprinkler systems;
- Maintenance of temperature and humidity levels;

- Avoidance of food and drinks in storage areas;
- Protection of records from ultraviolet light from sun and fluorescent lighting;
- Proper preparation of records for permanent storage;
- Records in formats other than paper.

The procedures should also ensure that when eligible records with a disposition of "Permanent Record" become inactive or are not regularly referenced, they are properly transferred to an archives.

### **Creation and implementation of a disaster recovery plan**

A disaster can disrupt the normal and continuous operations of the organisation. Examples of disasters are: fires, floods, hurricanes, tornadoes, earthquakes, electrical surges and power outages, burst water pipes, and computer viruses. The organisation should have a written disaster plan that includes a section on records. Prior to writing the plan, the organisation should:

- Identify vital and other valuable records critical to the functioning of the organisation (vital records are essential for conducting business);
- Ensure vital records are protected or duplicated before a disaster occurs;
- Identify structural, logistical, or other vulnerabilities to which records are exposed and overcome such vulnerabilities.

The actual disaster plan should be practical, clear, supported by management, and distributed to all those who are expected to respond to a disaster. Response procedures for each type of foreseeable disaster or emergency should be listed.

### **Training Staff**

Finally, once records management policies and procedures are created and adopted, it is important to train all staff members in their implementation and to ensure that staff members follow the policies and procedures. Following training, staff members should be held accountable for their records management activities.

*Oyedokun Ayodeji Oyewole is the president of Records and Information Management Awareness Foundation (RIMA Foundation), a Not-for-profit NGO that seek to promote proper management and security records and information for the benefit of the society and humanity. He can be contacted at: [president@rimaw.org](mailto:president@rimaw.org)*