Government of Saskatchewan Records Management Requirements for Business Systems[1]

Purpose

Government organizations must ensure that their public records remain accessible, retrievable, legible and transferable until they can be destroyed or transferred to the Provincial Archives of Saskatchewan (PAS) as per *The Archives and Public Records Management Act* (APRMA). In addition, in accordance with *The Electronic Information and Document Act* and *The Evidence Act,* public records in electronic form have to be preserved in a manner that ensures their integrity and authenticity. As more and more government business is conducted within a digital environment, it is necessary for Information Technology (IT) systems to incorporate records and information management (RIM) elements that will allow institutions to carry out their RIM functions within those environments in compliance with the applicable legislation and PAS's RIM policies.

This guideline provides a set of common RIM functional requirements for the design, development, and deployment of any IT business system including emails. The functional requirements have been developed by the RIM stakeholders working group in consultation with the Information Technology Division of the Ministry of Central Services to ensure that adequate RIM functionalities exist to support appropriate level of control over public records (structured or unstructured) maintained in IT business and email systems. The requirements do not need to be met purely within the business system in question, and may be met through the use of additional tools such as third party software or an external records management (RM) system provided the business system poses a capability to work seamlessly with the third party software and RM systems.

RIM Basics

In order to effectively utilize RIM functionalities of IT business systems, a government institution must have in place an approved records schedule(s) and a set of RIM policies and procedures (e.g. storage, transport, disposal procedures, etc.). The records retention and classification requirements included in the approved schedules and the applicable RIM policies have to be communicated to IT prior to the business system is being implemented so the system can be configured accordingly. IT may also find this information useful in establishing their maintenance and migration strategies.

Separate procedures may have to be developed for long-term records to ensure their integrity is preserved and that they remain understandable and useable (i.e. can be accessed, retrieved and read/viewed/listened to) for the period of time determined in the schedule. In addition, when applying records schedules, it is necessary to take into account the fact that the retention periods are based on the year of file closure unless specific conditions are defined.

[1] Based on the "Recordkeeping (RK) Functional Requirements for IT Systems", created by the Information, Privacy and Archives Division of the Ministry of Government and Consumer Services, Ontario, with permission.

Some records do not fall under the definition of a government record and are not subject to the RIM requirements included in the *APRMA* (see The Transitory Records Guidelines for me information: http://www.saskarchives.com/sites/default/files/pdf/transitory_rec_guide_fin.pdf).

Email Records

Email is a particular concern for records and information management. Many people are using MS Outlook as a *de facto* records management system for government email records by keeping most or all of their emails within Outlook and not applying records classification or properly disposition. In order to manage email, users currently need to either print and file or export emails out of Outlook and into a structured network drive.

The current email and network drive system has several problems that need to be addressed in any new system that is implemented in the future:

- There is currently no built-in method to label records with a records classification
- Moving records into the network drive is cumbersome and time consuming
- Emails are attached to a specific account and can be difficult to access once that account is closed (employee leaves position)
- There is no way to identify duplicate emails across accounts (e.g. "CC" or "BCC" copies)
- Metadata regarding email's sender, date received, etc. is not easily available outside of the email client
- Emails cannot be linked to related records outside of the client without exporting a copy of the email

RIM Functional Requirements

Records Creation and Capture

Functionalities that relate to a need to document business transactions which involve the creation and capture of records and associating them with their business context through metadata.

1. Ensure that business records created or received by the business system can be captured and stored along with associated metadata in a tightly inextricable and meaningful way, so that they can be managed as a single object during the entire retention of the record as per an approved records schedule.
2. Ensure each record is uniquely identifiable.
3. Be able to identify the business owner of a record, or the primary owner where records belong to multiple program areas.
4. If a record is made up of more than one component (e.g., email with attachments, dynamic webpages), the business system must be able to capture and maintain all components in a meaningful way, as either linked or a single object, as well as associated metadata during the entire retention of the record.
5. Where the business system supports the conversion of records from their native formats (e.g., .doc) to a format compatible with the system as part of the capture process (e.g., .pdf), it must ensure that the content, structure and context of the original records are properly retained as much as necessary to maintain the integrity of records.

6. Where the business system supports the capture, identification and/or transmission of encrypted records it must be able to maintain cryptographic keys for the entire authorized retention of the record with which they are associated.

Records Maintenance and Control

Functionalities that ensure records authenticity, reliability, integrity and usability and include metadata capture.

7. Be able to classify and safeguard business records with respect to their sensitivity in accordance with applicable access and security policies.
8. Be able to support a range of metadata elements and accommodate future metadata standards required to support business needs.
9. Be able to capture and manage metadata documenting key records lifecycle events (e.g., creation, significant alteration) and records management activities (e.g., disposition) from the creation of records to the end of their retentions. The metadata could include date, time, and the individuals, organizations and/or system processes responsible, for example disposition approval date.
10. Be able to automatically capture/update metadata as much as required directly from the authoring application, the operating system, the external records management system or the business system itself.
11. Be able to prevent unauthorized entering, update, or deletion of metadata.
12. Be able to draw together and provide access to all metadata elements for a record or a group of records governed by the same records series.
13. Be able to use the contents of certain metadata elements (e.g., date of record's creation) to determine and carry out a records management activity (e.g., final disposition) automatically.
14. Where the business system supports the encryption of records, it must be able to allow encryption to be removed when it is transferred to the Provincial Archives of Saskatchewan.
15. Where the business system supports the use of digital signatures, the system must support the use of metadata for records transmitted or captured bearing digital signatures to, at a minimum, note the fact that a digital signature was authenticated.
16. Be able to conduct detailed search functions that include elements such as:
    a. Full document text
    b. Metadata elements (subject line, classification, date created, etc.)
    c. Linked elements (e.g. email attachments)
17. Be able to produce reports, such as:
    a. all records series currently defined in the system;
    b. all records to which a particular records series is currently applied;
    c. all duplicate copies of a given record;
    d. all records subject to disposition holds.

Import/export Interoperability

Functionalities that support records import and export between systems, conversions (if necessary) for migration to newer technologies and transfer to PAS.

18. Accept the following components and elements (if provided by the importing system) and maintain the integrity of the imported records:
    a. in their existing file formats;
    b. associated metadata;
    c. proper relationships between components of records;
    d. proper relationships between records; and
    e. audit trail information (if any).
19. Be able to export business records to an external system (e.g. a records management system, a new system) or the Provincial Archives of Saskatchewan.
20. Ensure that each export action includes the following components and elements and ensure the integrity of the exported records:
    a. records in their existing file formats;
    b. associated metadata;
    c. proper relationships between components of records;
    d. proper relationships between records; and
    e. audit trail information (if any).

Classification, Retention, and Disposition

Functionalities that ensure that records remain accessible and usable to authorized users for a period of time stated in an approved and applicable schedule and that records can be destroyed or transferred to the Archives.

21. Throughout the record's authorized retention,
    a. ensure the integrity, reliability and authenticity of the record;
    b. ensure the record can be retrieved, accessed;
    c. ensure the record can be understood in a meaningful way; and
    d. prevent any unauthorized modification, deletion, or final disposition of the record.
22. Provide mechanisms to allow authorized users to define / update / delete retention and disposition rules in accordance with governing records series to a record or a group of records:
    a. a trigger to initiate the retention period (for example end of calendar year of records closure);
    b. a retention period to establish how long the record must be maintained.
23. The group of records assigned with the same records series must be linked together in a way that records management processes (e.g., retention, disposition) can be applied to all records within the group.
24. Be able to support rescheduling of governing records series whenever authorized and ensure records remain correctly assigned and records governed by the same records series are linked properly following the series rescheduling. This includes applying classification to unclassified records as well as systematically re-classifying records if a new records schedule is adopted to replace an existing one.
25. Support the application of multiple disposition actions (e.g. destroy, transfer, hold for appraisal).

26. Where the business system allows multiple governing records series, the system must be able to identify any conflict of retentions and disposition actions, notify the authorised users and request remedial actions if necessary.
27. Ensure that changes to either records series or assignment of records series take immediate effect on all records to which the (new) records series has been applied.
28. Be able to make records that are due for disposition fully available to the authorized disposition reviewers and approvers, including institutions outside of the GOS network such as PAS.
29. Ensure that no disposition action (destruction or transfer to the Archives) can be executed prior to final approval from authorized disposition approvers including the Provincial Archivist.
30. Only allow authorised users to execute disposition actions.
31. Be able to report on the outcome of a disposition action, detailing the records that are successfully destroyed or transferred and identifying those that were not successfully disposed.
32. Ensure that destruction results in the complete obliteration or inaccessibility of records (including all components of each record and associated metadata), and that the records cannot be restored through operating system features or specialized data recovery techniques.
33. Distinguish between an ad hoc deletion function and the destruction function within the disposition process, and prevent the delete function being used within the final disposition process, so that the final destruction of identified records can only be achieved through the controlled disposition mechanism of the system.
34. Document all disposition actions and retain the documentation for the retention specified in the appropriate records schedule (e.g. Administrative Records Management System, 2014 – Series 1525). The documentation should include information clearly describing the records including the inclusive dates, the applicable records classification schedule and records series, disposition approvals (including PAS's) and disposition action, and when and by whom the destruction is conducted.
35. Allow a disposition hold to be placed on, updated or removed from a record or a group of records by authorized users whenever needed or during the disposition review process.
36. Ensure the integrity, authenticity, retrievability and readability of the records and prevent any disposition action and deletion from taking place for the entire duration of the hold.
37. Support multiple holds being placed on a record or the same group of records at the same time.