Records Management

Alex Sverdlov
alex@theparticle.com

1 Introduction

In the course of running a business, data elements are generated. Some of these are deemed important enough to be designated as "records"—with the rest categorized as "non-records".

Records need special treatment: they must be preserved in approved locations, they must not be altered throughout their life, and they must be destroyed in accordance with record destruction policy that the company sets in place.

There are several corporate roles that oversee the definition, storage, and destruction of records. These often include the "data owner", who is the individual responsible for overall records strategy, and "records manager", who are individuals responsible for managing and enforcing the records management policies in respective domains/departments.

2 Records vs Non-Records

Each organization has their own definitions, but generally records include important business transactions.

For example, every interaction with the customer (irrelevant of how that interaction took place), would often be considered a record. Internal voice-mail may or may not be considered a record, depending on the organization, etc. Email almost always treated as a "record".

Copies of records, or drafts, are often non-records, etc.

3 Immutable

Records are immutable—and should be stored/treated that way. Alteration to a record must create another record (preserving the original record).

4 Approved Storage

Records must be kept in a location that is "approved"—which often means it has to be resiliant to failure. This almost always excludes drives on employee machines, or any portable media. The approved locations are often replicated and have very low failure rates.

5 Scheduled Destruction

The approved location is not only for resiliency. It's also for implementing proper record destruction process.

Normally, records are held for N years, where N is 5 or 7 years. Legal (or other) "holds" may prevent destruction of specific records: once the holds are lifted, the records go back to the default destruction policy.

Some records may be marked to never be destroyed. These are often public statements/announcements that the company is distributing externally. These often include social media posts, etc. The idea is that if someone other than the company may have a copy of it, then the company better have a copy of it too.

It is important that the record destruction policy is followed: storage is cheap, and the argument is often made to never erase anything. This may be simpler to implement, but it opens the doors to legal discovery—the company needs to be able to definitely say whether certain records exists or not, without conducting an expensive search.

6 Privacy Classification

Privacy classification enables application of policies to various records. These are often:

- Public: no restrictions on access. This does not mean the general public can access the records, just that the company doesn't take precautions with the data. These often include job postings (employees are not prevented from emailing details to their friends, etc.)
- Internal: the records/data should stay within the company. Employees should not be emailing this information outside the company. These may include department policies, etc.
- Classified: trade-secret information that should not be shared with anyone who is not cleared. Often these records are accessible within a respective department, and are not widely available within the organization.
- Personal: information that has personally identifiable details. This includes HR information about employees, and personally identifiable information about customers (names, addresses, etc.)

Besides these categories, there might be other ones specific to various industries, such as HIPAA.

Category often implies or requires certain storage type (encrypted), notifications (notify data owner whenever someone is accessing the data, etc), and retention (is it often not permitted to make copies of classified records on portable devices).

7 Management

This whole process of records management needs to be managed: which often includes defining policies, conducting training sessions (annual, quarterly, etc.) to ensure employees are aware of and follow the policies. Evaluating data storage locations and records management products.