The Sedona Guidelines for Managing Information & Records in the Electronic Age (2007)

This publication harmonizes the legal, policy, and technical considerations that bear on and should be considered by every public and private organization in today's electronic age. In particular, this publication sets forth "guidelines" to help organizations assess their unique needs and responsibilities in managing electronic information and records. Supporting each guideline is detailed commentary and citations to case law and pertinent trade literature to assist organizations in addressing these issues.

In terms of structure, these guidelines focus on two distinct situations involved in the management of electronic information and records. The first, and the bulk of the document, is comprised of guidelines that address the statutory, regulatory, and other legal obligations needed to manage and retain valuable information as an ongoing business matter. See Guidelines 1–4. The second addresses the responsibilities triggered by actual or reasonably anticipated litigation and government investigation when all types of relevant information must be preserved, regardless of whether that information has been identified as "records." See Guideline 5.

1. **An organization should have reasonable policies and procedures for managing its information and records.**
   a. Information and records management is important in the electronic age.
   b. The hallmark of an organization's information and records management policies should be reasonableness.
   c. Defensible policies need not mandate the retention of all information and documents.
2. **An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.**
   a. No single standard or model can fully meet an organization's unique needs.
   b. Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.
   c. An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.
   d. An organization should assess the operational and strategic value of its information and records in developing an information and records management program.
   e. A business continuation or disaster recovery plan has different purposes from those of an information and records management program.
3. **An organization need not retain all electronic information ever generated or received.**
   a. Destruction is an acceptable stage in the information life cycle; an

organization may destroy or delete electronic information when there is no continuing value or need to retain it.

b. Systematic deletion of electronic information is not synonymous with evidence spoliation.
c. Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice mail.
d. Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.
e. Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.
f. Absent a legal requirement to the contrary, organizations are not required to preserve metadata; but may find it useful to do so in some instances.

4. **An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.**
   a. Information and records management policies must be put into practice.
   b. Information and records management policies and practices should be documented.
   c. An organization should define roles and responsibilities for program direction and administration within its information and records management policies.
   d. An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.
   e. An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.
   f. An organization should consider the impact of technology (including potential benefits) on the creation, retention and destruction of information and records.
   g. An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.
   h. An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.
   i. Policies and procedures regarding electronic management and retention should be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy

rights or obligations.

j. Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.

5. **An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.**

   a. An organization must recognize that suspending the normal disposition of electronic information and records may be necessary in certain circumstances.

   b. An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.

   c. An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.

   d. An organization's information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.

   e. Legal holds and procedures should be appropriately tailored to the circumstances.

   f. Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program.

   g. Documenting the steps taken to implement a legal hold may be beneficial.

   h. If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.

   i. Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (i.e., there is no continuing duty to preserve the information), organizations are free to lift the legal hold.

The full text of *The Sedona Guidelines for Managing Information & Records in the Electronic Age* is available free for individual download from The Sedona Conference website at https://thesedonaconference.org/publication/Guidelines_for_Managing_Information_and_Electronic_Records.