A. Principles For Document Management Policies

Arthur Anderson, LLD v. U.S., 544 U.S. 696 (2005) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business . . . . It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.")

Lewy w. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (in reviewing whether documents destroyed pursuant to an existing retention policy constituted sanctionable conduct, court should determine whether the length of retention is reasonable given the particular type of document, whether lawsuits that would require production of these types of documents have been filed and their frequency, and whether the document retention policy was instituted in bad faith)

Hynix Semiconductor, Inc. v. Rambus, Inc., No. C-00-20905 RMW, 2006 WL 565893 (N.D. Cal. Jan. 5, 2006) (finding no spoliation or bad faith in implementation of document management and destruction policy because litigation was not "probable" at the time the party introduced the policy, as the "path to litigation was neither clear nor immediate" at that time)

1. **Document Management Policy:** written guidelines, published to relevant employees, that provide direction on the creation, storage, organization, retention, and destruction of business records and information.

2. **Ground-Up Design.** Policies should be designed from the ground up, based on institutional use and experience, rather than being based on potentially unrealistic and inapplicable notions arriving top down from management or legal departments.

3. **Driven By Business Needs.** Policies should not be "litigation driven" document destruction policies. Policies should codify business needs, requiring neither more nor less. Business needs should guide setting maximum retention periods (destruction dates).

4. **Constrained By Applicable Law**. Likely applicable statutes of limitations, and statutory and regulatory retention periods should guide setting minimum retention periods. Identify and list the statutes and regulations applicable to the company's work, and periodically update them. Where a litigation track record exists, identify the statutes of limitations typically encountered in the company's litigation.

5. **Standardized Hold Procedures For Predictable Recurring Litigation.** Where recurring forms of litigation can reasonably be expected, document retention standards and procedures can be designed in advance, avoiding the need to design new litigation holds for each new matter.

6. **Policy Development Is Documented.** The process of developing the policy should itself be well-documented, since courts consider the circumstances of a policy's development in determining whether sanctions should be awarded if the policy results in destruction of potential relevant material.

7. **Consider An Enterprise Document Management System.** Enterprise document management systems are designed to retain documents in a way that allows them to be found when needed for litigation, without the input of the users who created the documents.

8. **Identify The Key Types Of Business Records.** Policies should identify the various types of business records typically created by the organization, using terms that will be clearly intelligible to those expected to implement the policy.

9. **Create An Enterprise Information Model.** The model describes the types of systems that contain these various types of business records, and identifies the custodians of these systems. The model increases the speed and reduces the cost of locating potentially relevant business records when a duty to preserve arises.

10. **Create a Data Library For Litigation.** Always a work in progress, the data library should be a readily searchable repository of qualitative and quantitative information on each node of the Enterprise Information Model, including:

a. What types of Electronically Stored Information ("ESI") are "inaccessible," both technologically and because of the burden and expense in accessing them, with specific, documented factual bases for those conclusions

b. Current, quantified cost data to support burden testimony

c. What types of preservation (*e.g.*, interruption of disaster recovery tape recycling, individual hard drive imaging) the company will challenge if sought by an adversary, with data on why it is unreasonable to preserve such ESI

d. The categories of ESI contained on disaster recovery tapes and the technological ability (if any) to search those tapes for specific ESI or the ESI of specific personnel

e. All case management reports, discovery responses and objections, affidavits, deposition transcripts, and court filings that include information on the company's ESI, to help ensure consistency and preservation of institutional knowledge and create efficiencies in discovery response

f. A listing of all litigation holds that have been put in place by the company, including the nature, location, and status of all data that has been held

B. Guidance On Litigation Holds

Pension Committee of the University of Montreal Pension Plan v. Bank of America Securities, LLC, 685 F. Supp. 2d 456, 471 (S.D.N.Y. 2010) ("After a discovery duty is well established, the failure to adhere to contemporary standards can be considered gross negligence. Thus, after the final relevant *Zubulake* opinion in July 2004, the following failures support a finding of gross negligence, where the duty to preserve has attached: to issue a written litigation hold; to identify all of the key players and to ensure that their

electronic and paper records are preserved; to cease the deletion of email or to preserve the records of former employees that are in a party's possession, custody, or control; and to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources.")

Rimkus Consulting Group, Inc. v. Cammarata, 688 F. Supp. 2d 598, 613 & n. 9 (S.D. Tex. 2010) ("It can be difficult to draw bright-line distinctions between acceptable and unacceptable conduct in preserving information and in conducting discovery, either prospectively or with the benefit (and distortion) of hindsight. Whether preservation or discovery conduct is acceptable in a case depends on what is *reasonable*, and that in turn depends on whether what was done – or not done – was *proportional* to that case and consistent with clearly established applicable standards….For example, the reasonableness of discovery burdens in a $550 million case arising out of the liquidation of hedge funds, as in *Pension Committee*, will be different than the reasonableness of discovery burdens in a suit to enforce noncompetition agreements and related issues, as in the present case.")

Orbit One Communications, Inc. v. Numerex Corp., 2010 WL 4615547 (S.D.N.Y. Oct. 26, 2010) ("Indeed, under some circumstances, a formal litigation hold may not be necessary at all. Rather than declaring that the failure to adopt good preservation practices is categorically sanctionable, the better approach is to consider such conduct as one factor, and consider imposition of sanctions only if some discovery-relevant data has been destroyed.")

1. **Litigation Hold**: A repeatable, documented process for satisfying the company's duty to preserve information for litigation and regulatory proceedings.

    a. The goal is to establish processes to identify, locate, preserve, retrieve, and produce potential relevant information.

    b. The substance of the litigation hold must be adequately communicated to employees

    c. This communication should include a two-step process in which (1) basic information about the litigation hold is broadly communicated within the organization, and (2) more detailed information and focused efforts to preserve and gather information are provided to "key players" identified as especially likely to have information relevant to a particular litigation.

    d. Communication of the litigation hold is followed up, (1) broadly, through periodic reminders, to accommodate turnover in the organization, and (2) specifically, as new "key players" are identified in the course of investigation and discovery.

    e. Data collected pursuant to these processes should be stored on a special litigation database server that is independent of normal system operations and backups.

    f. Fact finding and investigation in litigation should consistently include appropriate efforts to investigate and identify the locations reasonably likely to contain unique and relevant electronically stored information.

g. This investigation should include reasonable steps to ascertain whether orphaned or legacy data contain relevant information.

h. In ongoing litigation, the company should take steps to secure relevant, unique electronically stored information that would otherwise be overwritten or deleted by automatic processes.

i. This process may include search terms, date ranges, and specific mailboxes to allow searches to be run and the results archived in a litigation database which remains available as the master source for searching and production of documents throughout the litigation.

2. **The Duty To Preserve.** The obligation to preserve business records, including ESI, requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information. *See The Sedona Principles: Second Edition* 28 (June 2007).

3. **Reasonable Balancing.** But a reasonable balance must be struck between (1) an organization's duty to preserve relevant evidence, and (2) an organization's need, in good faith, to continue operations. *Id.; see* Fed. R. Civ. P. 37(f) (Absent exceptional circumstances, a court may not impose sanctions under the Federal Rules of Civil Procedure on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system).

4. **When The Duty To Preserve Arises.** When "a party reasonably anticipates litigation, it has a duty to suspend, as to documents relevant to the anticipated litigation, any routine document purging system that might be in effect; failure to do so constitutes spoliation." *Rambus, Inc. v. Infineon Techs. AG*, 222 F.R.D. 280, 288 (E.D. Va. 2004).

5. **The Scope Of The Duty To Preserve.** The duty to preserve extends to information that the party knows, or reasonably should know, will likely be requested in reasonably foreseeable litigation. *Mosaid Techs., Inc. v. Samsung Elecs. Co.*, 348 F. Supp. 2d 332, 336 (D.N.J. 2004).

6. **Active Systems First.** Rule 26(b)(2)(B), Federal Rules of Civil Procedure, explicitly limits initial discovery of electronically stored information to information from reasonably accessible sources. Reasonably accessible sources generally include files available on a computer user's desktop, or on a company's network, in the ordinary course of operation. *The Sedona Principles: Second Edition* 18 (June 2007).

7. **Litigation Servers.** Collecting data on a special litigation database server that is independent of normal system operations and backups is advisable. Litigation servers can more easily be isolated from document destruction routines. Litigation servers are easier to secure against modification or destruction of information. Litigation servers can assist in maintaining a chain of custody, where necessary.

8. **Proactive Meeting And Conference**. Parties to litigation should meet and confer as early as practicable to discuss the scope and parameters of the preservation obligation.

9. **"Key Player" Identification.** Likely witnesses should be identified early and their information, documents, and, where appropriate, systems, can be gathered and preserved.

10. **Keyword Searching.** When practicable, active systems should be searched using key words relevant to the subject matter of the proceeding to isolate information to be preserved for later review. Whether or not the preserved material eventually needs to be searched or produced, this undertaking can avoid the need to completely suspend routine document destruction procedures, while still satisfying the duty to preserve. See Zubulake V, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (concluding that system-wide keyword searches for electronic documents relevant to pending or anticipated litigation should have been run to ensure such documents were preserved from deletion pursuant to a document retention policy where an archive system was in place).

11. **When Extraordinary Efforts May Be Required.** The obligation to preserve normally requires reasonable and good faith efforts. The obligation to undertake extraordinary efforts should be exercised only when there is substantial likelihood that the information exists; that it would not remain in existence absent intervention; that the information (or its substantial equivalent) cannot be found in another, more accessible data source; and that its preservation is likely to materially advance the resolution of the litigation.

12. **Not Readily Accessible.** Information is "not reasonably accessible" where obtaining it would cause undue burden or cost, such as retrieving electronically stored information from backup tapes that are intended for disaster recovery purposes and are not indexed, organized, or susceptible to electronic searching; legacy data that remains from obsolete systems and is unintelligible on the successor systems; and data that was deleted but remains in fragmented form, requiring computer forensics to restore and retrieve it. Resorting to disaster recovery backup tapes and other sources of electronically stored information that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing the electronically stored information from such sources, including the disruption of business and information management activities. *The Sedona Principles: Second Edition* 45 (June 2007). "[A]s a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation. . . . However, it does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of 'key players' to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available." *Zubulake IV*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003).

13. **Sanctions, Prejudice, and Culpability.** Sanctions, including spoliation findings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant ESI, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party. Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 746-47 (8th Cir. 2004) (adverse inference instruction should not be given on the basis of negligence alone; there must be a finding of bad faith or some other culpable conduct, such as the ongoing destruction of documents during litigation

and discovery even after they have been specifically requested). However, some courts treat failure to follow established litigation hold best practices as "gross negligence" sufficient to constitute the requisite culpability, and will allow relevance and prejudice to be rebuttably presumed from that gross negligence. See Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 542-53 (D. Md. 2010) (providing chart collecting cases on major topics including whether proportionality concept is incorporated into required culpable state of mind).

14. **Actions In Good Faith.** Federal Rule of Civil Procedure 37(f) now incorporates the good faith standard, stating that a sanction should not issue if electronically stored information is lost as a result of the "routine, good-faith" operation of an electronic information system. Good faith has both subjective and objective aspects in the context of electronic discovery. Considerations of a party's "good faith" may include the following inquiries:

a. was there a standard litigation hold process and was it followed?

b. did the party adequately communicate litigation hold instructions to employees?

c. did the party periodically distribute litigation hold reminders?

d. did the party adequately investigate and identify the locations that were reasonably likely to contain unique and relevant ESI?

e. has the party been cooperative and forthcoming in Rule 26(f) and Rule 16(b) discussions

f. has the party been reasonable and forthcoming in written discovery responses and depositions?

g. did the party take steps to secure relevant, unique ESI that would otherwise be overwritten or deleted by automatic processes?

h. did the party take reasonable steps to ascertain whether orphaned or legacy data contain relevant information?

i. was the electronic system designed and implemented solely with the intent of meeting