

small_frog/Getty Images

Drafting a Document Retention Policy

A document retention policy establishes and describes how a company expects its employees to manage company information from creation through destruction, and is a crucial part of a company’s overall records management program. Counsel must understand the key issues involved in developing an effective document retention policy to ensure the policy complies with applicable laws and is tailored to the company’s specific legal and business needs.



VICTORIA A. REDGRAVE
CHAIR, EXECUTIVE COMMITTEE
REDGRAVE LLP

Victoria is Chair of the firm’s Executive

Committee. She previously served as in-house litigation counsel for two major corporations and as general counsel at a technology company. Victoria is a member of The Sedona Conference Working Group on Electronic Document Retention and Production and the Seventh Circuit Electronic Discovery Pilot Program.



JONATHAN M. REDGRAVE
MANAGING PARTNER
REDGRAVE LLP

Jonathan is a founding partner of the firm. He has extensive experience

in all areas of complex litigation in both state and federal courts and focuses his practice on information law, including electronic discovery, records and information management, and data protection and privacy issues. Jonathan is Chair Emeritus of The Sedona Conference Working Group on Electronic Document Retention and Production.



LISA A. LUKASZEWSKI
COUNSEL
REDGRAVE LLP

Lisa has extensive experience advising clients on information

governance, e-discovery, and data privacy issues in business and litigation environments. She is a member of the International Association of Privacy Professionals, ARMA International, and The Sedona Conference Working Groups 1 and 6.

A document retention policy (DRP) (also referred to as a records and information management policy, a recordkeeping policy, or an information governance policy) provides the framework for a company's records and information management program. An effective DRP:

- Provides direction to company personnel on how they should manage information created or used in the course of the company's business operations.
- Safeguards a company's records and proprietary information, which consequently helps the company manage and reduce operational, reputational, and litigation risks.

When developing a DRP, counsel must take into account the company's particular legal and business needs, including:

- The company's:
 - industry;
 - geographical location;
 - structure;
 - culture; and
 - technological environment.
- The types of information the company maintains.
- The manner of information flows inside and outside the company.

In addition to evaluating the company's specific needs, when drafting a DRP, counsel should consider:

- The key objectives of the DRP.
- Guidelines provided by leading authorities on information management.
- Practical steps to help ensure effective implementation of the DRP.



Search [Document Retention Policy](#) for a sample DRP, with explanatory notes and drafting tips, and [Document Retention Policy: US Checklist](#) for more on the considerations and steps involved in drafting a DRP.

OBJECTIVES OF A DRP

The main objectives of a DRP are to:

- Explain the key terms and concepts underlying the DRP.
- Instruct employees about company information subject to retention requirements.
- Outline the roles and responsibilities of employees as they relate to the DRP.

EXPLAIN KEY TERMS AND CONCEPTS

When drafting a DRP, counsel should clarify concepts that are critical to understanding the DRP. Employees must appreciate that information is a vital company asset that must be appropriately managed throughout its lifecycle, which includes both retaining and disposing of information in accordance with the DRP.

In particular, the DRP should:

- Explain that company records are owned by the company and highlight the importance of records management.
- Identify who is responsible for managing the records program.
- Clearly delineate employee records management responsibilities.
- Describe the consequences of non-compliance.

Additionally, the DRP should define key terms using common, nontechnical language wherever possible, including the meaning and significance of:

- Records.
- Disposable information.
- Records retention schedules.
- Litigation holds.

When drafting definitions, counsel may find it useful to check with employees who are not DRP specialists to help ensure that the definitions are clear and widely understandable.

Records and Disposable Information


For employees to appropriately manage company information, they must be able to distinguish between:

- **Records.** Records reflect information that is created, transmitted, or received in the course of company business that the company wants, or is required, to retain for business or legal purposes (see below *Identify Information Subject to Retention Requirements*). A company must retain information for the length of time specified in the company's records retention schedule (see below *Records Retention Schedules*) where the information:
 - serves as the company's corporate memory of an action, a decision, or a statement;
 - has enduring business value (for example, where the information provides a record of a business transaction, evidences the company's rights or obligations, protects the company's legal interests, or ensures operational continuity); or
 - must be retained due to legal, accounting, or other regulatory requirements, including records that are subject to one or more litigation holds.
- **Disposable information.** Disposable information is all company information that is not a record as defined in the company's DRP. Disposable information should ordinarily be discarded or deleted once it no longer serves a useful business purpose and there is no other requirement mandating retention of the information. However, a company must retain disposable information that is subject to a litigation hold, even when it no longer serves another temporary useful purpose (see below *Litigation Holds*).

In addition to explaining the distinctions between different types of information, a DRP should reinforce the idea that these categories are media-neutral. In other words, the DRP should clearly define records and disposable information to include

information in paper or electronic format, as well as physical objects. For example, in a manufacturing context, a sample widget may constitute a research and development or quality assurance record. Similarly, information in database fields may constitute records.

Further, the DRP should recognize and reflect that destruction is an important stage in the lifecycle of both records and disposable information. As the US Supreme Court noted in *Arthur Andersen LLP v. United States*, destruction of information pursuant to a “valid” DRP is “not wrongful” under “ordinary circumstances” (544 U.S. 696, 703-06 (2005)). The standard for evaluating a company’s actions under a DRP (and whether those actions may result in sanctions) is governed by Federal Rule of Civil Procedure (FRCP) 37(e), as amended on December 1, 2015, which makes clear that the sanctions provision “does not apply when information is lost before a duty to preserve arises” (2015 Advisory Committee’s Note to FRCP 37(e)).

 Search [Sanctions in Federal Court Toolkit](#) for a collection of resources to help counsel understand, avoid, and seek sanctions in federal civil litigation and arbitration.

Records Retention Schedules

Records retention schedules are a simple way to instruct employees on how long they must keep company records. Typically, a records retention schedule is a series of charts that lists in separate columns:

- **The categories of records a company creates, receives, or uses in the ordinary course of business.** This information is organized by department, business process, or function. The records retention schedule should name or describe the record categories with sufficient detail to allow employees to identify which category applies to a certain record.
- **The length of time the company must retain each record category.** Retention time periods are often based on a combination of legal and business factors.

A basic retention schedule may use the following format:

RECORD	RETENTION PERIOD
Personnel Records	
I-9 Forms	The later of 3 years after hiring or 1 year after separation
W-2 and W-4 Forms	As long as the document is in effect + 4 years
Corporate Records	
Articles of Incorporation, Bylaws, Corporate Seal, Minute Books	Permanent

 Search [Document Retention Policy](#) for a sample records retention schedule, with explanatory notes and drafting tips.

Some records retention schedules include additional information, such as the departmental owner of the information or additional requirements regarding the storage, management, or disposal of the records.

If applicable, a records retention schedule should include both the minimum and maximum time limits for retaining records. Maximum retention periods are imposed by law, contract, or another external source and indicate the longest amount of time the company may retain the information. Though uncommon, some US laws specify maximum retention periods. For example:

- The Utah Employment Selection Procedures Act requires disposing of job applicant data within two years of when the applicant provides the information to the employer, unless the applicant is hired (Utah Code § 34-46-203(2)).
- The federal Video Privacy Protection Act requires the destruction of a customer’s video rental records within one year from the date the information is no longer necessary for the purpose for which it was collected (18 U.S.C. § 2710(e)).

Maximum retention periods more commonly arise outside the US, especially in Europe. For example, the General Data Protection Regulation (GDPR), which became effective in May 2018, sets out a general policy that personal data should be retained only as long as required for the legitimate purpose for which it was gathered. If a maximum retention period is not specifically defined by law, statute, or regulation, a record should be retained for the minimum time period established by the company as set out in the records retention schedule and then destroyed within a reasonable time after that period expires. (For more information on the GDPR, search [Overview of EU General Data Protection Regulation](#) on Practical Law.)

Regardless of the expiration of the applicable retention periods, a company must keep records that are subject to a litigation hold until the hold is lifted and no longer applicable to the records at issue.

Litigation Holds

If a company is involved in or reasonably anticipates becoming involved in litigation (including arbitration), a government investigation, or an audit, it must ensure that relevant information is neither deleted nor destroyed. Accordingly, companies should develop a litigation hold policy that requires the suspension of normal destruction practices for records and disposable information that are related to the litigation, investigation, or audit. A litigation hold, or similar procedures, also may be used in other exceptional circumstances requiring the retention of information beyond its ordinary period, such as a merger, a divestiture, or an acquisition, or following a settlement, sanction, or judgment.

Typically, employees within a company’s legal department should be responsible for deciding when to implement a litigation hold and making other decisions required while the litigation hold is in place. In companies without a legal department, the chief operations officer or head of the information technology (IT) group should make those decisions with the assistance of outside counsel when needed. A company usually implements

a litigation hold by issuing a litigation hold notice (also known as a legal hold notice or document preservation notice) to those employees who may have relevant records or information.



Search [Litigation Hold Notice](#) for a sample litigation hold notice, with explanatory notes and drafting tips.

When drafting a DRP, counsel should consider specifically defining the term “litigation hold” as an action undertaken by the company to preserve records and information that are related to an existing or a reasonably anticipated lawsuit, government investigation, or audit that:

- Suspends the ordinary destruction and disposal of records and disposable information.
- Overrides the retention periods set out in the records retention schedule for records that are subject to the litigation hold.

By including a clear and precise definition of a litigation hold in the DRP, and by plainly describing in the litigation hold notice the types of records and information that employees must retain, counsel can help to ensure employees do not accidentally destroy records and information that the company has a legal duty to retain.

Further, should the company need to defend its preservation actions, these clear definitions and descriptions may bolster the company’s position on the reasonableness of its preservation efforts. If the company loses information that should have been retained, the presence and effectiveness of a litigation hold are likely to factor into a court’s analysis on whether to issue any sanctions (FRCP 37(e); see, for example, *Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135, 162 (2d Cir. 2012) (noting that the adoption of appropriate preservation practices is one factor in the analysis of whether to issue sanctions)).

Additionally, counsel should consider whether to include in the DRP:

- A litigation hold policy. If the litigation hold policy is not integrated into the DRP, the DRP should refer to it and make clear to employees that implementing a litigation hold suspends ordinary record and information destruction procedures related to the affected records and information.
- A description of the steps counsel and employees must take to carry out the litigation hold so that records and information subject to the hold are not discarded while the hold remains in place.
- Specific information about litigation hold implementation, given that the DRP generally is not protected by the attorney-client privilege (for more information on the attorney-client privilege, search [Attorney-Client Privilege and Work Product Doctrine Toolkit](#) on Practical Law).



Search [Litigation Hold Toolkit](#) for a collection of resources to help counsel preserve documents and implement a litigation hold.

IDENTIFY INFORMATION SUBJECT TO RETENTION REQUIREMENTS

Designing an effective DRP involves identifying the types of information that the company should retain, typically by listing these types of records in a records retention schedule (see above *Records Retention Schedules*). To assess the types of records a company may need to retain and for how long, counsel should consider two broad categories of information, namely information that the company:

- Should retain for internal business reasons because the information has a long-term business value for the company.
- Must retain for legal or other external reasons.

Information Retained for Internal Business Reasons

Certain information holds long-term intrinsic operational or strategic value to the company, such as information that:

- Memorializes decisions and activities.
- Informs future decisions and activities.
- Allows the company to secure or defend its rights.

A company should retain this information while it has sufficient value to the business and that value outweighs the costs and risks of retaining the information. The assessment of whether and how long to retain information should reflect the perspective of multiple business stakeholders, including the business users of the information and the business functions that incur the cost of storing and managing the information (including costs associated with infrastructure, litigation and discovery, and disposition of the information).

Information Retained for Legal or Other External Reasons

Certain information, regardless of its internal business value, may be subject to retention requirements arising from:

- Federal and state laws and regulations.
- Contracts.
- Sanctions.
- Other external requirements that affect how long the information must be (or can be) retained.

External requirements may be:

- **Set out explicitly.** These include requirements imposed by regulation or contract. For example:
 - the Occupational Safety and Health Administration (OSHA) requires most employers with 11 or more employees to retain logs of work-related injuries and illnesses for at least five years (29 C.F.R. §§ 1904.1, 1904.29, 1904.33) (for more information, search [OSHA Injury and Illness Recordkeeping](#) on Practical Law); and
 - the Employee Benefits Security Administration requires the person or entity responsible for administering a company-sponsored employee benefit plan subject to the Employee Retirement Income Security Act of 1974 (ERISA) to retain any records that must be disclosed under ERISA for at least six years from the date on which they were required to be disclosed (29 U.S.C. § 1027).

- **In the form of guidance.** Examples include regulatory agency opinion letters, position statements, and auditor procedures.

As discussed above, companies also must preserve records and information that are relevant to an ongoing or a reasonably anticipated lawsuit, government investigation, or audit involving the company (see above *Litigation Holds*). However, this is handled by issuing a litigation hold instead of by listing these records and information in a records retention schedule.

DEFINE EMPLOYEE DRP ROLES AND RESPONSIBILITIES

A DRP should outline employee responsibilities arising from the DRP and define the roles and groups within the company that are in charge of implementing and managing the DRP. The DRP may include or link to appendices that assist employees with meeting their obligations under the DRP, such as:

- Key contact information.
- Records retention schedules.
- Records storage procedures.
- Procedures for the disposition and destruction of inactive records.
- Procedures for handling the records of separated employees.

The DRP should address the roles and responsibilities of:

- All company employees generally.
- Records coordinators within each business unit or department.
- The records and information management committee tasked with supervising DRP administration.
- Other key employees, depending on the company.

All Employees

Employees create, receive, and use company information in their daily business and are primarily responsible for managing that information. The DRP should clearly indicate that it is every employee's responsibility to properly maintain and dispose of records and disposable information consistent with the company's DRP and records retention schedules, as well as to comply with other records management procedures, such as storage or naming conventions.

Supervisors should ensure that employees and third parties that create or use the company's records or information comply with the company's DRP and records retention schedules.

Records Coordinators

Typically, records coordinators (also known as records managers) are individuals within a company designated by a departmental head to:

- Oversee retention and disposal of records and information within a particular business unit or region.
- Assist their business unit or region's employees in complying with the DRP.

Records coordinators often function as the company's first line of defense in ensuring DRP compliance. Therefore, they

must have specific knowledge of the relevant records and information issues and the particular retention requirements for their business unit or region. Because records coordinators are embedded within particular business units or departments, they are often the first to identify specific records and information management challenges. Also, they are usually best positioned to quickly answer questions from colleagues and anticipate DRP issues before they become a problem.

Records and Information Management Committee

A records and information management committee is a designated group tasked with:

- Supervising the administration of the DRP.
- Making decisions on adopting and modifying records retention schedules.
- Regularly reviewing and revising the DRP as needed to keep it current.
- Strengthening the company's information management program.
- Responding to questions about how to implement the company's information management program.

Typically, the records and information management committee is made up of employees from the compliance, legal, information security, and IT departments. This ensures that all DRP stakeholders are involved when DRP decisions are being made. The records and information management committee should also include senior-level employees, enabling the committee to make most DRP-related decisions without requiring additional layers of approval.

Other Employees

In addition to the individuals and roles described above, the DRP may need to address the roles of:

- **The corporate records manager.** Some companies employ a corporate records manager who handles the day-to-day DRP operations and liaises with the records coordinators, the business units or departments, and the records and information management committee. The corporate records manager, however, needs the active involvement and cooperation of other employees to properly manage the company's records and other information.
- **Individuals responsible for making decisions related to a litigation hold.** As discussed above, this responsibility may rest with the company's legal department employees, chief operations officer, or head of the IT group (see above *Litigation Holds*).

INFORMATION MANAGEMENT FRAMEWORKS

Counsel should consider consulting standard information management frameworks when developing a DRP. The Sedona Conference and ARMA International are the two leading authorities on information management. The resources they provide emphasize that companies must develop their own DRPs and information management programs customized to their:

- Industry.
- Legal profile.
- Geographies.
- Workforce.
- Culture.
- Technology infrastructure.
- Information flows.

The Sedona Conference and ARMA International best practices are explained below.

THE SEDONA GUIDELINES

The 2007 edition of *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* (2d ed.) (Sedona Guidelines) provides helpful tips that counsel should consider when developing a DRP. In particular, counsel should make sure the company:

- Adopts reasonable policies and procedures.
- Develops a DRP that is realistic, practical, and customized to the company.
- Incorporates procedures to avoid the unnecessary retention of all electronic information.
- Takes a comprehensive approach to the information lifecycle.
- Mandates the suspension of ordinary destruction practices and procedures to comply with any litigation holds.

Adopt Reasonable Policies and Procedure

A company's information management policies and procedures should:

- Make sense in relation to the company's circumstances.
- Be easy to understand.
- Not blindly mandate the retention of all information and documents.

Make the DRP Realistic, Practical, and Customized

Because no model policy can fully meet all of a company's unique operational, regulatory, and IT needs, there is no single template that accommodates every company's circumstances. Counsel should:

- Evaluate operational, strategic, and legal issues to understand the value of information for retention.
- Ensure the DRP is sufficiently flexible and scalable to meet the needs of the company's various layers and groups.
- Distinguish retention requirements under the DRP from retention requirements under the company's business continuation or disaster recovery plan.

Do Not Unnecessarily Retain All Electronic Information

Companies may systematically destroy information that is not required to be retained for legal reasons. In general, unless special circumstances exist, companies may:

- Adopt programs that regularly delete emails, instant messages, text messages, and voicemails.

- Recycle backup media.
- Systematically delete or destroy residual or shadowed data.
- Set standards for what metadata will be generated in the ordinary course of business and whether it will be retained.

Take a Comprehensive Approach

An effective DRP should take into account the various issues that arise throughout the information lifecycle, which involves the creation, identification, retention, retrieval, and destruction of information. Counsel should take steps to:

- Implement the necessary retention policies and schedules.
- Document information management practices, including those that may not be included in the DRP.
- Define DRP roles and responsibilities for program direction and administration.
- Guide employees on how to identify and maintain information that has a business purpose or must be maintained by law or regulation.
- Define the roles and responsibilities of content and technology custodians for electronic records management.
- Address the impact of existing and new technologies (including the potential benefits and risks) on the creation, retention, and destruction of records, such as the use of:
 - both company-owned and personal mobile devices; and
 - third-party services, infrastructures, or platforms.
- Educate employees about the specific terms and provisions in the DRP.
- Conduct periodic compliance reviews of DRP procedures and respond to the findings of those reviews as appropriate.
- Coordinate the DRP with other policies concerning the use of company property and information, including applicable privacy rights or obligations.
- Implement a continuous evaluation process to update policies and practices, as needed, in response to changes in:
 - workforce;
 - company structure;
 - business practices;
 - legal or regulatory requirements; or
 - technology.

Provide for a Litigation Hold

The Sedona Guidelines explain that a DRP may include instructions on how the company suspends ordinary destruction practices when necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigations, or audits. As discussed above, DRPs often include these types of instructions or reference a separate litigation hold policy containing them (see above *Litigation Holds*).

Developing these instructions requires counsel to:

- Anticipate circumstances that require a litigation hold and have a plan in place to implement a hold that is tailored to the company.

- Address how to effectively communicate notice of a litigation hold, provide necessary training, and document the steps taken to implement the hold.
- Identify employees with the authority to suspend normal destruction procedures and impose a litigation hold.

Counsel should note that it is also important for the litigation hold process to include procedures for returning the “suspended” content to the DRP’s normal information management procedures after the hold has expired.



Search [Litigation Hold Lift Notice](#) for a sample litigation hold lift notice to alert recipients that a litigation hold is no longer in effect, with explanatory notes and drafting tips.

ARMA INTERNATIONAL’S GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES®

ARMA International’s Generally Accepted Recordkeeping Principles (the Principles) are another helpful guide to understanding the issues counsel should consider when developing a DRP. The Principles can be summarized as follows:

- **Principle of accountability.** The company should assign a senior executive to:
 - oversee the recordkeeping program;
 - delegate responsibility for the recordkeeping program to appropriate individuals;
 - adopt policies and procedures to guide employees; and
 - ensure the recordkeeping program’s auditability.
- **Principle of integrity.** The recordkeeping program should be devised so that the records and information the company generates, receives, and manages have a reasonable guarantee of authenticity and reliability.
- **Principle of protection.** The recordkeeping program should be designed to ensure a reasonable level of protection to records and information that are:
 - private;
 - confidential;
 - privileged;
 - secret; or
 - essential to business continuity.
- **Principle of compliance.** The recordkeeping program should comply with:
 - applicable laws and other binding authorities; and
 - company policies.
- **Principle of availability.** The company should maintain its records in a way that ensures the timely, efficient, and accurate retrieval of needed information.
- **Principle of retention.** The company should maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.

- **Principle of disposition.** The company should securely and appropriately dispose of records it no longer needs to maintain.
- **Principle of transparency.** The company should document its recordkeeping processes and activities in a way that all employees and appropriate parties can understand them.

ARMA International’s website ([arma.org](#)) also provides information and links to resources regarding the international records management standard, ISO Standard 15489-1:2016, which sets out high-level guidance and best practices on designing information management programs and can be a useful checklist in creating DRPs (see, for example, Nancy Dupre Barnes, *ISO 15489 – Revised and Redesigned for 2016*, Information Management, Sept./Oct. 2016, at 30, available at [imm.arma.org](#)).

PRACTICAL CONSIDERATIONS

An effective records management program recognizes that a company’s DRP is not a stand-alone document. Instead, the DRP incorporates other policies related to records and information retention, such as policies on:

- Computer use (for more information, search [IT Resources and Communications Systems Policy](#) on Practical Law).
- Personal device use (for more information, search [Bring Your Own Device to Work \(BYOD\) Policy](#) on Practical Law).
- Information security (for more information, search [Information Security Policy](#) on Practical Law).
- Social media use (for more information, search [Social Media Policy \(US\)](#) and [Company Social Media Use Guidelines](#) on Practical Law).
- Data privacy (for more information, search [Privacy Compliance and Policies Toolkit](#) on Practical Law).

Additionally, companies developing a DRP should:

- Proactively make sure that employees comply with the DRP.
- Instruct employees on how to integrate the DRP’s processes and requirements into their daily tasks.
- Update the DRP regularly.

COMPLIANCE

Companies must mandate employee compliance with the DRP. A company should explain to employees that a comprehensive and mandatory records and information management program exists and take steps to measure compliance. Clearly communicating the need for all employees to strictly comply with the DRP requires strong language, such as the following:

“All company employees must comply with this policy, the records retention schedules, and any litigation hold communications. Failure to do so may subject the company, its employees, and contract staff to serious civil and/or criminal liability. Failure to comply with this policy may result in disciplinary sanctions, including dismissal or contract termination.”

RECORDS MANAGEMENT TOOLKIT

The Records Management Toolkit available on Practical Law offers a collection of resources to help counsel manage a company's records and other data. It features a range of continuously maintained resources, including:

- [SEC Record Retention Schedule](#)
- [Implementing a Litigation Hold](#)
- [Creating and Maintaining Employee Personnel Files Checklist](#)
- [The Dodd-Frank Act: CFTC Swap Data Reporting and Recordkeeping](#)
- [Immigration Document Retention Chart](#)
- [Non-Profit Records Retention and Destruction Policy](#)
- [Document Retention: Presentation Materials](#)
- [How to Organize Company Data Before Litigation Arises Checklist](#)
- [Document Retention and Disposal Policies](#)
- [CFTC Record Retention Schedule](#)

However, the company should not commit to stern warnings in writing unless it is willing and prepared to undertake compliance and enforcement actions.

Additionally, a company may implement an audit program, which allows the company to measure and demonstrate employee compliance with the DRP. Audits can take many forms, such as focusing on employee awareness or reviewing actual practice. Audits should assess both retention and disposal of records and information, as well as compliance with litigation holds.

RECORDS MANAGEMENT DOCUMENTATION AND EDUCATION

For DRPs to be effective and consistently applied throughout a company, the company should provide employees with:

- An easily accessible resource that documents the DRP procedures.
- Regular training and education on how to implement the DRP procedures, especially when the DRP is updated or revised.

Ideally, the DRP, records retention schedule, program documentation, and education and training materials will be separate documents. This helps ensure that the DRP remains mostly static, while regular updates to other records management documentation are applied as the company changes its internal systems and processes.

Documentation

Typically, documentation of a records and information management program describes how to implement the DRP and related procedures in the company's particular information and business environment. For example, the program documentation may instruct employees on:

- How to use the company's document management system or software.
- Proper procedures for sending paper records to offsite storage, including appropriate labeling and indexing.
- Proper methods for disposing of information that no longer serves a useful purpose or records that have reached the end of their retention period.

- Whom employees should contact when questions about the DRP arise.

Education and Training Materials

Records and information management education and training materials instruct employees on how to comply with the requirements of a company's DRP. These materials may be part of a company's human resources, IT, security, or business ethics policies. A company should present these materials in connection with its:

- Orientation procedures for new employees.
- Learning curriculum in a company university, where virtual or in-person class attendance is required and tracked.

Training materials should include instructions on how to comply with a litigation hold notice, as well as how to properly destroy records that have met their required retention period. For example, the training manual may state that all hard copies of financial and employee-related records must be shredded when they are no longer required to be held under either the company's records retention schedule or a litigation hold.

UPDATES TO THE DRP

To maintain the accuracy of a company's DRP, counsel should:

- Review the DRP at least once each year.
- Re-publish updated versions of the DRP as needed.
- Distribute the updated DRP company-wide, highlighting the changes and how they affect employees' daily tasks.

The authors wish to thank Karen O. Hourigan, Michael Kearney, and Kenneth A. Prine for their contributions to previous versions of this resource.