

## How to Structure a Plan for E-Discovery

This resource guide provides a model structure for company’s “E-discovery Playbook”. With plaintiffs’ lawyers so alert to opportunities to challenge the credibility of corporate defendants, this playbook becomes a vital resource for ensuring that key considerations are taken into account, hopefully before a major discovery project is required.

Various parts of this playbook can be developed or assembled by members of the e-discovery team. For some companies with smaller law departments, it may be very sensible to assign the development of this playbook to a law firm that already works closely with the department that has strong knowledge about the company’s electronic document environment. An expert e-discovery consultant might also play this role.

Playbook Section	Focus Summary
<b>E-Discovery Team</b>	<ul style="list-style-type: none"> <li>• Designated team members and contact information</li> <li>• Roles and responsibilities of records managers in company business and corporate units</li> <li>• Roles and responsibilities of outside counsel</li> </ul>
<b>Document Retention Policy Inventory</b>	<ul style="list-style-type: none"> <li>• Copies of the document retention policy or policies being observed by company units</li> <li>• Analysis of pertinent reasons for the differences in policies being used</li> </ul>
<b>Technology Environment Analysis</b>	<ul style="list-style-type: none"> <li>• Inventory of technology environments, systems and location and status of electronic materials</li> </ul>
<b>Pertinent Legal Issues and Analysis</b>	<ul style="list-style-type: none"> <li>• Identification and analysis of legal issues relevant to various technology systems and considerations</li> </ul>
<b>Communication and Training Plan</b>	<ul style="list-style-type: none"> <li>• Briefing for legal department staff on salient factors they should understand</li> <li>• Plan for educating IT staff about legal issues and for educating legal staff about IT issues</li> <li>• Plan for training the business staff</li> </ul>
<b>Materials for Submission to the Courts</b>	<ul style="list-style-type: none"> <li>• Materials prepared in advance to be tailored to each case that arises</li> </ul>
<b>Vendor Analysis</b>	<ul style="list-style-type: none"> <li>• Profiles of selected vendors, with contact information, with preliminary determination of when each should be used</li> </ul>
<b>Procedures Upon Notification of Discovery</b>	<ul style="list-style-type: none"> <li>• Steps to be implemented when a discovery demand is received</li> </ul>

<b>Demand</b>	
<b>Evergreen Strategy</b>	<ul style="list-style-type: none"><li>• Designated people responsible for updating the Playbook document</li></ul>

## **I. Designated E-Discovery Team**

- Lead attorney and other attorneys
- Project manager for this case or group of cases
- Document retention supervisors (corporate and business units)
- Business unit liaison(s), especially those designated as records managers
- HR Department liaison
- IT lead executive and lead IT managers for the various computer environments or business units
- Designated outside counsel litigation and discovery expert(s)
- Preferred e-discovery vendor(s)

## **II. Inventory of Document Retention Policies**

- Copies of all document retention policies currently in place at corporate or in business units
- Description of the business units and business locations addressed by each policy (policies may vary by location as well as business unit)
- Contact information for those responsible for supervising each policy (including after-hours contact information) and their backup supervisors
- Analysis of the differences in the policies and the reasons for the differences (perhaps a table or matrix)
- Narrative history of the development and implementation of each policy (e.g., the implementation of the policy when the BU was owned by a different company)
- History of problems that have arisen during any prior document discovery activities, including use of vendors, spoliation issues, etc.

## **III. Technology Environment Analysis**

- Document on-line data and file storage systems by major types of applications (e-mail, customer history file, document management, etc.)
- Document back-up policies and procedures
  - Inventory back-up and off-line data storage systems and identify whether the systems are "obsolete"

- Identify physical storage locations and conditions (e.g., whether materials are in the control of third parties such as outsourcing vendors) and the notification requirements for obtaining them
- Determine whether the inventory of data backup and file storage materials conforms to the inventory's log description
- Audit backup and file storage materials in relation to standards set forth by document retention policies to identify discrepancies (and correct any inaccuracies)

#### **IV. Pertinent Legal Analysis**

- Identify any e-discovery standards applied by judges to the specific types of technology systems currently or previously used in your environment
- Analyze how these standards might be applied to your situation
- If appropriate, prepare arguments that different standards should apply
- Identify any electronic records stored beyond policy retention standards not currently under hold orders that could / should be destroyed -- implement appropriate steps

#### **V. Communication and Training Plan**

- Convene an e-discovery team meeting to:
  - Review results of foregoing activities
  - Develop a common understanding of e-discovery issues
  - Identify appropriate action steps to be implemented
- Meet with legal department management and staff to brief them on:
  - Preparations of the e-discovery team
  - Legal and technology developments that will affect the company's posture in any future e-discovery proceeding
  - Any recommendations for appropriate policies and actions steps
- Develop and implement legal issues briefing for appropriate IT managers throughout the company
- Develop training program for IT personnel who will appear in court (when required) to describe IT activities and respond to questions
- Develop and implement technology issues briefing for legal staff and outside counsel
  - Develop and implement training program for the business staff

- Schedule periodic meetings of the e-discovery team to discuss legal and technology developments and resolve issues that arise

## **VI. Materials For Possible Submission to the Court**

- Description of the specific IT environment(s) related to the discovery order including: computer systems, including servers, networks, e-mail systems, voice mail systems, databases, desktop and laptop computers, PDAs, and backup and archival tapes or other similar storage media
- Description as to whether relevant and discoverable electronic data may arise in third party storage or processing entities such as internet storage or servicing facilities
- Description of changes in made in the company's systems during recent years and any information as to the existence of any relevant and discoverable electronic data which is not located on currently used electronic devices (legacy data)
- Appropriate description of document retention policies and practices for areas of the company subject to discovery order
- If applicable, explanation of the disparate retention policies and practices in various business units
- Description of corporate structure and operations
- Arguments supporting the company's view of the appropriate e-discovery standards that should apply in light of the company's IT policies and practices
- Arguments supporting the company's view that the costs for some portions of the e-discovery costs should be shifted to the requesting party
- Estimates provided by vendors to process data as required by the initial discovery order, particularly that typically defined as "inaccessible" in accordance with the Zubulake order
- In anticipation of overly onerous document preservation orders from the court, arguments for narrowing the court's order for document preservation to those which are truly relevant to the case

## **VII. Vendor Analysis**

- Identify and profile recommended vendors best qualified to manage e-discovery projects of various types (based on interviews if possible)
- Document vendor contact information
- Execute confidentiality agreements and prepare orientation materials for vendors to familiarize them with the company's IT environments, legal and other considerations

- Develop stand-by project agreements to be used with vendors on short notice
- Pre-clear the vendors with IT personnel so that rapid access to technology facilities and systems is not delayed when e-discovery activities need to commence on short notice
- Pre-screen and register recommended vendors with company procurement units to ensure rapid engagement on short notice

### **VIII. Procedures Upon Document Discovery Notification**

- Designation of specific project manager(s)
- Notifications to IT staff and their subsequent steps to confirmation their activities and understanding (Hold Order)
- Notifications to company employees and confirmation procedures (Hold Order)
- Notifications to e-discovery vendors
- Initial e-discovery team meeting
- Review of possible legal steps to narrow discovery order(s)
- Tailoring of materials to be submitted to the court
- Determination of discovery project milestones and deadlines

### **IX. Evergreen Strategy**

- Designate people accountable for updating specific sections and documents in the Playbook to keep all sections reasonably current
- Identify the intervals at which sections and documents are to be updated
- Assign responsibility to a project manager to monitor and report on the timeliness of updates
- Monitor the job assignments of team members and appoint replacements and new team members when circumstances warrant

### **Common Mistakes**

- Failure to have one person who is the primary designated leader to supervise all e-discovery projects

- Failure to achieve very close coordination with the law firm or firms working on the case to ensure that identical standards and methods are being applied to every aspect of the project by all legal counsel
- Failure to consult with an electronic evidence expert before starting to collect and evaluate potentially responsive electronic documents
- Failure to use vendor(s) that do have truly state-of-the-art technology systems for accelerating and improving the quality of document review and production
- Failure to adequately train IT staff to understand and properly address court expectations and legal requirements from the outset
- Failure to plan adequately to avoid unnecessary duplication of time and cost in managing the e-discovery process
- Failure to have practice “walk throughs” of the plan before it has to be used in an actual major case – *every plan has weaknesses that should be addressed*
- Failure to initiate the document collection, imaging and coding process early enough in the litigation process
- Failure to ensure that the document search process is broad enough to ensure that all responsive electronic data and documents are identified and collected