

*This is a sample approach to developing a sound document collection process, referenced in Section C(7)(b)(vii) (“Collection and review of hard copy documents and ESI”), page 22 of the Guidelines on Best Practices for Litigating Cases Before the Court of Chancery. It should be modified to fit the circumstances and used in conformity with the Guidelines.*

- I. Preservation.
  - A. Identify and record steps taken to preserve potentially relevant information, *i.e.*, information that is known (or reasonably should be known) to be relevant in the action.
  - B. Preservation is not limited to simply avoiding affirmative acts of destruction because day-to-day operations routinely alter or destroy evidence.
  - C. Parties are not required to preserve every shred of information. Act reasonably. If possible, seek agreement with the opposing parties at the beginning of the litigation about steps to take to preserve potentially relevant information and how to handle the privilege assertion process.
  
- II. Issue Initial Litigation Hold Notice.
  - A. Review document retention and destruction policies.
    - 1. Determine what practices must be suspended.
    - 2. Follow litigation hold process (if any) outlined therein unless you determine it is insufficient.
    - 3. Consider need for amended or supplemental litigation hold notices as litigation develops or as new individuals or issues are identified.
    - 4. Consider sending periodic reminders of litigation hold notices.
  - B. Promptly send litigation hold notices to the custodians identified as sources of potentially relevant information.
    - 1. Take conservative (broad) view of relevant issues and custodians.
    - 2. Err on the side of inclusiveness.
  - C. Litigation hold notice should:
    - 1. Be circulated as soon as all parties are aware of the potential for litigation, and potentially in the engagement letter if litigation is contemplated at the time that counsel is engaged.
    - 2. Specifically state that potentially relevant information and records must be preserved.
    - 3. Identify general and specific categories of potentially responsive information.

- D. Discontinue use of any ephemeral messaging applications that automatically delete messages once a party has read/opened them (e.g., Snapchat and TigerText).
  - E. Discontinue any "recycling" of relevant former employees' computers, tablets and smart phones.
  - F. Identify and properly preserve (if necessary) relevant backup tapes in response to the litigation hold notice (e.g., earliest available backup, backup from day of preservation request and any other particularly relevant backups).
  - G. Document steps taken to implement litigation hold (e.g., preserve any litigation hold notices that have been issued; create a checklist outlining the steps taken from the point of notice through the decision to release the hold; any other method that tracks compliance with hold instructions).
- III. Formulate a Protocol or Plan to Identify and Properly Collect Potentially Relevant Information.
- A. Goals:
    - 1. Establish legal and technical strategies for data gathering, review, and production.
    - 2. Comply with legal obligations including potential evidentiary issues.
    - 3. Minimize expense and burden.
    - 4. Be prepared to explain and defend the process.
      - (a) Carefully document all data identification and collection efforts.
      - (b) Identify and enable a discovery response coordinator or liaison to describe information custodians, systems, storage, retention policies and collection process.
  - B. Practice Tips:
    - 1. Discovery is a collaborative and iterative process that should involve a number of individuals, including but not limited to, outside counsel, inside counsel, IT, Data Privacy/Security, records management, business unit personnel and consultants/vendors, if necessary.
    - 2. Consider interviewing:
      - (a) General Counsel.
      - (b) Chief Information Officer.
      - (c) Director of Information Technology.

- (d) Technology support personnel.
- (e) Records management personnel.
- (f) Disaster recovery personnel.
- (g) Data Privacy or Security Officer.
- (h) HR Director (for potential personnel changes).
- (i) Individuals who are likely to be key witnesses.

IV. Identify Potentially Relevant Information.

- A. Take reasonable steps to identify sources of potentially relevant information.
- B. Determine scope and type of potentially relevant information.
- C. Find out how information is generated, maintained and destroyed in the normal course of business.
- D. Identify key witnesses and custodians, as well as their administrative assistants or other persons maintaining their documents, if applicable.
- E. Identify custodians with potential privileges (*e.g.*, attorneys).
- F. Determine relevant time frames.
- G. Prepare keyword lists.
  - 1. Relevant jargon, acronyms or code names can be used to assist with processing and review of data.

V. Determine the Information Management Landscape.

- A. Map information systems to obtain accurate picture of data sources.
  - 1. Practice Tip: Consider obtaining a general diagram from the client's IT network administrator depicting the types and locations of servers deployed throughout the organization.
  - 2. Identify the document management systems.
  - 3. Identify the e-mail systems.
    - (a) Identify the email administrator.
    - (b) Identify the types of e-mail systems.

- (c) Assess any encryption or password protection issues.
  - (d) Identify potential for remote access and means that were used.
  - (e) Determine whether users archive e-mail outside the mail server on their local drives, other network locations, or removable media.
- B. Review document retention/destruction policies.
  - 1. Assess the extent of automatic deleting or archiving both for email and the network generally.
  - 2. Confirm whether the litigation hold has been implemented properly.
- C. Determine what happens to former employees' e-mail, computers, tablets, smart phones and documents when they leave the company.
  - 1. Determine whether the practices have changed over time.
  - 2. Determine whether they have been suspended or exceptions created for relevant former employees.
- D. Address backup media and disaster recovery systems.
  - 1. Determine type, procedure and schedule.
  - 2. Prepare a list of the servers that are backed up.
  - 3. Determine whether any system changes occurred during the relevant time period.
- E. Determine the need for forensic data capture.
  - 1. Have any types of activities occurred that would require the forensic copying of hard drives or servers?
  - 2. Have files been deleted or written over that may be potentially relevant?
- F. Evaluate legacy systems.
  - 1. Assess the need to access legacy systems.
  - 2. Determine whether the necessary hardware, software or technical expertise to access legacy data exists within company.
  - 3. If the necessary expertise is not available within the company, determine whether it is available from consultants, and at what cost.

- G. Consider offsite or third-party systems:
1. Cloud computing systems.
  2. Off-site company storage facilities.
  3. Co-location data centers.
  4. Third party data warehousing.
  5. Third party data tape storage.
- H. Determine the Company's schedule for any future upgrades, data migration or data consolidation that might affect the ability to utilize currently available data or recently archived data.
- I. Identify any additional sources of potentially relevant information, such as the following:
1. Local workstations or laptop hard drives.
  2. Public/Private servers.
  3. A central Storage Area Network (SAN).
  4. Removable media (*e.g.*, CD-Roms, DVDs, zip drives, thumb drives, flash drives, external hard drives, etc.).
  5. Digital voice mail stores and/or VOIP (voice over internet protocol) stores.
  6. Cell phones (including text messages), personal digital assistants, portable media players, tablets, and/or other mobile devices.
  7. Intranets/extranets.
  8. Central records/Off-site storage facility.
  9. Home computers.
  10. Failed drives from which a forensic recovery might be possible.
  11. Social media (*i.e.*, Facebook, Instagram, LinkedIn, Twitter or other similar programs)
  12. Messenger or text messaging platforms or applications (*i.e.*, Google Chat, Microsoft Teams, Facebook Messenger, AOL Instant Messenger, WhatsApp, TigerText or other similar programs)

- J. Consider discussing with the client, if applicable to the nature and size of the case, the potential for using technology or computer assisted review software.