HAMPTON VA

No. IT– 135	Policy Name: E-Discovery Policy
Effective Date: 7-1-2011 Last Revised Date: 6-23-2014	Citywide Policy _ IT Policy _ IT Procedure X
Approved By: IT Director	

Purpose: To ensure that e-Discovery Requests and Litigation Hold Notices are received, routed and responded to in a timely and thorough manner.

Policy:

1) e-Discovery Requests (Request) and Litigation Hold Notices (Notice) must be responded to within a timeline determined by the City Attorney's Office;
2) Receipt of a Request or Notice must be acknowledged within twenty-four (24) hours;
3) Notices may require the active participation of department data owners who must segregate and maintain Electronic Stored Information (ESI) for the duration of the Hold;
4) The City is expected to be responsive while guarding against creating an overwhelming volume of material to be searched.

Procedure: This procedure is designed to provide an informed and reasoned approach to e-Discovery requests and to ensure that the City's actions facilitate discovery.

Section I: General Responsibilities

- City Attorney's Office
- Information Technology Department
- Department Data Owners
- Role of the Records Manager

Section II: Duty to Preserve

Section III: Responding to a Request

- Information Technology Department
- Department Data Owners

Section IV: Closing an e-Discovery request

Appendix A: Application Portfolio

Section I: General Responsibilities

The City Attorney's Office is responsible for:

- Being the official point of contact for all Requests, Notices and ESI produced by the IT Department and Department Data Owners in the City.
- Communicating requests, and being available to Department Data Owners and the IT Department on any questions and clarifications on Requests or Notices.
- Maintaining and tracking all data provided by the IT Department and Department Data owners to ensure all data is received for any given request.
- Providing searchable information (filter(s)) specifically tailored for each Request or Notice (specific search words, terms and/or phrases).
- Establishing a timeline for receipt of ESI for Requests and/or Notices.
- Providing Notices and instruction to City Employees who may hold ESI.
- Notifying the IT Department and Department Data Owners when a Request or Notice expires and that regular records management activities may resume.
- Review and ultimate disclosure of ESI in response to a Request or Notice. This includes ensuring that privileged, confidential, and non-responsive ESI are handled appropriately.

The Information Technology Department is responsible for:

1. Informing the CAO of the availability of ESI from City and other sources (databases and other software programs, email, specific departments, etc.).
2. Producing IT records and IT systems data in electronic form even if that same information has already been produced on paper.
3. Providing data storage for IT records and IT systems throughout the Request or Notice period.
4. Producing data in a form readable by another party's computers provided the format is one that the IT Department's standard systems' supports.
- Taking measures to preserve IT records and IT systems data throughout the Request or Notice process.

Department Data Owners are responsible for:

1. Providing the CAO with all relevant information on e-Discovery requests including user names and addresses, file locations, e-mail accounts, etc. to enable efficient e-Discovery searches.

1. In conjunction with the CAO, disseminating information to all relevant staff members and instructing them on e-Discovery request information, processes and specific tasks.
2. Informing the CAO of the availability of ESI from systems not managed by the IT department (relevant data on personal devices, servers and storage managed by the department, personal e-mail, storage devices containing data like thumb drives, etc.).
3. In conjunction with the CAO and IT, producing all responsive data and taking measures to preserve that data throughout the Request or Notice process.
4. Producing all responsive data and taking measures to preserve data throughout the litigation process

In the case of Department System Administrators (Police, etc.), management and administration of department data throughout the Request or Notice period will be required. This includes e-mail and other relevant sources of ESI throughout the Request or Notice period.

Role of the Records Manager

1. Requests and Notices received from the City Attorney's Office are routed to the IT Department Director and any appropriate department heads. The IT Department Director will route Requests and Notices to the Records Manager and any other applicable IT Department Staff members.
a. All Requests and Notices received by the IT Department must include names of specific individuals and phone numbers to facilitate a search of e-mail and phone records conducted by the IT Department.
b. The Records Manager will track Requests and Notices on behalf of the IT Department; include any relevant responses and forward responsive information to the CAO.

Department Data Owners are responsible for tracking requests received and maintaining relevant department data independent of the IT Department.

Section II: Duty to Preserve

Once the City reasonably anticipates litigation, and the CAO has put a Request or Notice in place, the IT Department and Department Data Owners must suspend routine records management activities (destruction, etc.), to ensure that preservation of relevant ESI occurs. Request and Notices will be disseminated by the CAO to specific City employees.

Records subject to a Request or Notice must be segregated, are not disclosable to the public until the Request or Notice, and are not subject to routine records management activities. Questions regarding records subject to a Request or Notice, including FOIA

requests, must be directed to the CAO; release of information must be authorized and approved by the CAO.

One exception to preservation are backup tapes maintained solely for the purpose of disaster recovery. These may continue to be recycled based on the City's practice of allowing the backup tape program to inform IT staff that tapes are no longer usable.

This specific activity does not limit availability of evidence. However, if the City can identify where particular employee documents are stored on backup tapes, then those tapes must be preserved if the information contained on those tapes is not otherwise available.

Section III: Responding to a Request

e-Discovery requests should include what electronic documents and data are being asked for, the scope and the limits of that data. Unclear requests must be clarified by the IT Director or Department Director prior to proceeding.

Information Technology Department:

The IT Department is not responsible for providing documentation on non-IT maintained systems and individual Department Data Owners outside of the IT Department (Appendix A).

Understand the composition of the source ESI. This means that IT staff will be responsible for determining if any document, file type, images without searchable text, etc., needs to be converted, translated or processed so it can be filtered.

Apply the filter supplied by the CAO (name, time period, address, etc.). The IT Department is responsible for applying the search terms (filter) supplied by the CAO. The CAO is responsible for evaluating the outcome of the search, or applying additional search terms upon receipt of the ESI.

Maintain Data Accountability. Clear documentation of what work was performed must be provided, including tools used and results. This means that the IT Department must maintain the identification of the original source of data (file location, directories, drive mappings, file counts for each unique source for each custodian). If specific types of ESI are not searched or included for review that should be documented. A custodian-based view would provide the total number of items from all sources. **IT Department Only:** This information (searches conducted (filters), tools used and results), must be provided to the Records Manager who will compile all documentation and forward to the CAO.

Exception processing. The IT Department is responsible for reporting where data exceptions occur. This may include password-protected, corrupted or unreadable ESI, and lost, damaged or stolen documents and files. Determining whether or not to inform parties regarding exceptions is the responsibility of the CAO.

Department Data Owners:

Department Data Owners must respond to the CAO independent of the IT Department.

Understand the composition of the source ESI. This means that Department Data Owners will be responsible for determining if any document, file type, images without searchable text, etc., needs to be converted, translated or processed so it can be filtered.

Apply the filter and evaluate the results. Department Data Owners are responsible for applying the search terms (filter) supplied by the CAO. The CAO is responsible for evaluating the outcome of the search.

Maintain Data Accountability. Clear documentation of what work was performed must be provided, including tools used and results. This means that Department Data Owners must maintain the identification of the original source of data (file location, directories, drive mappings, file counts for each unique source for each data owner). If specific types of ESI are not searched or included for review that should be documented. A custodian-based view (data owner view) would provide the total number of items from all sources.

Exception processing. Department Data Owners are responsible for reporting where data exceptions occur. This may include password-protected, corrupted or unreadable ESI, and lost, damaged or stolen documents and files. Determining whether or not to inform parties regarding exceptions is the responsibility of the CAO.

Information created or received throughout the Request or Notice period must be provided to the CAO within twenty-four (24) hours.

Section IV: Closing an e-Discovery request

Until departments have been instructed that the litigation hold is no longer in effect. All ESI pertaining to that the hold notice must be preserved even if newly created and provided to the CAO. The CAO is responsible for providing prompt information when a litigation hold is no longer in effect and departments are to comply with such termination notice.

Appendix A: Applications Portfolio
Attachment A: You just received an E-Discovery Request or Litigation Hold Notice
Attachment B: IT Department Documentation

Appendix A: Applications Portfolio

The IT Department maintains a listing of the major application systems being used by City Departments. Interdependencies between systems are mapped to show where these applications connect to other systems inside and outside of the City. Departments should refer to the IT portfolio in the Tech Manual found on the City Intranet under policies.

Attachment A You just received an e-Discovery Request or a Litigation Hold Notice

Any city staff member may at any time, receive a Litigation Hold Notice or an e-Discovery request. This means that you might have some electronically stored information (ESI) that could be relevant to current City litigation.

e-Discovery Request: Is a request for information in electronic format as part of the litigation process. ESI must be segregated and preserved for the duration of Discovery.

Litigation Hold Notice: Requires that the electronic information be segregated and preserved for the duration of the hold.

ESI includes e-mail, documents stored on your pc or the City's network, information on your mobile device, CDs and DVDs and flashdrives, etc. ESI could be information that you created or received from another source, it could also be part of a system, database or other application the City uses.

What should you do?

Review the Request or Notice within 24 hours and within that 24 hour period inform the CAO that you've received the Notice or Request, and search for any information you may have. If you need assistance conducting a search, please contact the CAO and the IT Department.

Call the CAO with any questions you have regarding the Hold, and ask for help if you need it.

If you receive a Litigation Hold Notice: Move *ALL* (or as much as possible) of the ESI that applies to the Notice into a separate folder on your shared network drive (this may include e-mail, correspondence, maps, etc) from all sources.

- This information must be kept separate for the duration of the Hold. It is not available to the public or other City staff and must be preserved.
- If the ESI is part of a larger system, database or application do not worry about separating it – that information will remain where it is currently stored.

Respond to the CAO with the information requested.

- This must be done in a timely manner and the CAO should provide you with a date that your response is required.
- If you have to provide any ESI to the CAO, keep it in electronic format – burn it onto a CD and deliver it personally to the CAO. Do not print the information.

If you receive a FOIA or other routine request for information that is under a Litigation Hold, please route the request to the CAO immediately for appropriate response.

Keep the ESI separate until the Litigation Hold is lifted. You will receive a notice from the CAO when a Litigation Hold has ended. Then you can return the ESI you have stored to its former folders, etc.

What should you NOT do??

You ***must not***
Disclose, Delete or otherwise destroy,

Or in any way alter ESI that is part of an e-Discovery Request or subject to a Litigation Hold

Attachment B: IT Department Documentation

The IT Department is not responsible for providing documentation on non-IT maintained systems or for individual department data owners outside of the IT Department.

The IT Department is responsible for providing documentation of e-Discovery ESI to the CAO that include the following information:

- Results of searches conducted
- Filter(s) applied
- Tools used
- Composition of source ESI if it cannot be immediately produced and any recommendation(s) to convert to allow filtering
- Any ESI not included, including exceptions that occur during filtering

Each group or individual in the IT Department who conducts searches for an e-Discovery Request must provide the above information to the Records Manager for compilation and forwarding to the CAO.