Category: Legal and Compliance Responsible Office: University Counsel	Procedure Title: Legal Proceeding Preparation (E-Discovery) Procedure Document Number: 6610 Effective Date: April 09, 2014 This procedure item applies to: State-Operated Campuses

Table of Contents

Summary

University officers, employees and agents who use electronic storage systems and programs must understand the basic operations of those systems and programs in order to manage records and "Electronically Stored Information" (ESI) according to applicable laws, regulations, policies, and retention schedules. This includes understanding the duty to notify "Counsel" of potential "Triggering Events."

The SUNY Office of General Counsel will make the ultimate determination of what constitutes a Triggering Event. Following such a determination, Counsel will issue a "Legal Preservation Notice," if necessary. Counsel will then direct the "Legal Hold" process and, if necessary, the subsequent production of ESI.

"Key Persons" must cooperate with Counsel to identify, preserve, maintain, and produce ESI that is subject to a Legal Hold, and "IT Personnel" must assist Counsel in the same.

In order to prepare for the significant burden and responsibility that E-Discovery can impose on a campus, the best practice is for each campus to form an E-Discovery Response Team. The E-Discovery Response Team will lead the campus-based efforts to comply with this Procedure.

Process

I. Purpose

The State University of New York is responsible for complying with various information demands made by the public, oversight agencies, adverse parties in litigation, and the courts. Such demands may arise in the context of litigation, administrative proceedings, audits, investigations, and Freedom of Information Law (FOIL) requests. With the proliferation of electronic information storage capabilities and systems, the task of complying with these requests has become ever more complicated and challenging. The purpose of this Procedure is to provide guidance to aid (state-

operated) University campuses, constituencies and officers in their efforts to prepare for and comply with "E-Discovery" responsibilities and demands.

II. Definitions

"*Counsel*" means any attorney of the University's Office of General Counsel ("OGC"). Generally, this will mean attorneys designated as "campus counsel" and at some larger campuses could encompass multiple attorneys working together. Where appropriate, Counsel may designate other officers to act on his or her behalf. When a matter has proceeded to litigation and the Attorney General's Office is involved, the assigned Assistant Attorney General may also direct the Legal Hold process. Occasionally other outside legal counsel may also be involved at the behest of OGC.

A "*Custodian*" is any officer, employee, or agent of the University who possesses, controls, or maintains any record, information, or data of the University.

"*E-Discovery*" is a short hand term for the process of preserving and exchanging ESI in the context of modern litigation or other legal processes.

"*Electronically Stored Information*" or "*ESI*" means any information, record, document, file or data that is stored electronically. ESI may include documents, audio recordings, videotape, e-mail, instant messages, text messages, word processing documents, spreadsheets, databases, calendars, telephone logs, contact information, Internet usage files, metadata, and all other electronic information created, received, and/or maintained on computer systems. ESI may reside on any University program, system, device, or server of any kind or in an employee's personal devices and accounts if such devices and accounts are used for conducting University business.

"*IT Personnel*" means the Chief Information Officer of any campus and his or her designees.

A "*Key Person*" is any University officer, employee, or agent who possesses, controls, or maintains any record, information, or ESI that is subject to a Legal Hold. A Key Person may also be someone who is in a position of leadership over a subject program or department (HR, Student Affairs, Facilities, etc.), or someone who has been designated as a campus liaison to Counsel.

A "*Legal Hold*" is the process by which the Office of General Counsel ("OGC") directs the preservation of certain records and ESI for the purpose of complying with a legal obligation. The basic steps to implementing a Legal Hold are:

1. All University officers, employees or agents *manage* records and ESI in accordance with SUNY records retention schedules and policies;
2. All University officers, employees or agents *notify* Counsel (or appropriate supervisor) of possible Triggering Events;
3. Counsel *determines* whether to implement Legal Hold;
4. Counsel works with Key Persons to *identify* the location of relevant ESI and other records;
5. Counsel *issues* Legal Preservation Notice;
6. Key Persons, IT Personnel, and Counsel (the E-Discovery Response Team) work together to *preserve* relevant records and ESI and plan for ongoing collection, if necessary;
7. Key Persons, IT Personnel, and Counsel *maintain* the Legal Hold until it is released;
8. Counsel notifies custodians when the Legal Hold may be released.

A "*Legal Preservation Notice*" is a set of written instructions that is sent from Counsel to Key Persons in order to initiate a Legal Hold. A Legal Preservation Notice may be issued electronically; however, it should include an appropriate acknowledgment of receipt. At a minimum, a Legal Preservation Notice should include information related to:

1. The nature of the Triggering Event giving rise to the Legal Hold;
2. The ESI or other records that are subject to the Legal Hold;
3. A brief recitation of the legal obligations related to Legal Holds in general;
4. Instructions for preserving the relevant ESI (including any transfer instructions);
5. Contact information for both legal and IT advice.

A "*Triggering Event*" is any event or set of circumstances that cause Counsel to reasonably anticipate litigation or another legal process that gives rise to a preservation obligation. Factors to consider in determining whether a Triggering Event has occurred include but are not limited to:

1. Likelihood of litigation or other legal processes, including communication from potential parties to a lawsuit or their representatives;
2. History of the institution related to a potential matter in dispute;
3. Location, durability, and control of potential ESI;
4. Media coverage;
5. Seriousness or magnitude of potential legal action;
6. Relative burdens and costs of preservation effort;
7. Common sense and professional judgment.

III. E-Discovery Response Team

A. Each campus should designate and maintain an E-Discovery Response Team consisting of Counsel (campus counsel), IT Personnel, the campuses' Records Management Officer (RMO), and other officers (such as Risk Managers) as suitable to the structure and personnel of the campus. The E-Discovery Response Team on each campus shall be charged with ensuring overall compliance with this Procedure and assessing, implementing, and monitoring the campuses E-Discovery processes.

B. The E-Discovery Response Team will oversee the actual E-Discovery projects from the time that Counsel determines a Triggering Event has occurred through preservation, review and, if necessary, production. This will typically include communication, oversight and management of the process.

C. Each member of a campus E-Discovery Response Team should be informed of ongoing and new E-Discovery projects on its campus and should take an active role in ensuring that the Key People involved in those projects understand their duties under this Policy.

D. Upon the initiation of any E-Discovery project, the E-Discovery Response Team should meet to discuss the necessary steps that must be taken and roles that individuals should play.

E. The E-Discovery Response Team should regularly report to the campus administration regarding current E-Discovery projects and compliance initiatives.

F. The E-Discovery Response Team should provide regular training to various campus constituencies in order to ensure that such constituencies are prepared for compliance with this policy.

G. Each campus should provide the E-Discovery Response Team with adequate resources and adequate authority to carry out its functions.

IV. Specific Duties

A. Counsel

1. Be familiar with campus and System ESI systems, including e-mail, word processing, spreadsheets and databases, student information, backup and archival systems, and websites.

2. Issue Legal Preservation Notice upon the occurrence of the following events:
    i. Receipt of administrative Complaint (e.g., EEOC, OCR, SDHR);
    ii. Receipt of NOI, Claim or Summons and Complaint;
    iii. Appeal of a disciplinary matter to arbitration;
    iv. Catastrophic events involving injury to persons or property.

3. Use best professional judgment to consider issuing a Legal Preservation Notice upon the occurrence of any event giving rise to a reasonable anticipation of litigation or another legal process for which ESI may be relevant. Such events may include:
    i. Initiation of investigation by state or federal law enforcement;
    ii. Initiation of investigation by Inspector General;
    iii. Receipt of Attorney Demand Letter;
    iv. Injury to persons or property;
    v. Major employment actions, such as tenure denial or the filing a grievance;
    vi. Major contract actions, such as breach or early termination;
    vii. Major student actions, such as dismissal or interim suspension;
    viii. Receipt of a FOIL request;
    ix. Audit by outside agency (e.g. OSC);
    x. Knowledge of litigation or investigation for which the University may become a real party in interest;
    xi. Receipt of a subpoena.

4. Once it is determined that a Triggering Event has occurred, work with applicable campus leadership and the E-Discovery Response Team to identify Key Persons.

5. Describe litigation facts and issues sufficiently to facilitate identification of relevant documents or information. Determine appropriate search terms or key words for use in search tools/software on an ongoing basis.

6. Identify the appropriate time period for the Legal Hold and determine whether the Legal Hold is continuing or only retrospective.

7. Define scope/types of ESI for recipients of Legal Preservation Notice. Provided that Counsel acts reasonably, Counsel need not take every conceivable step to preserve all available and potentially related data. Among the issues that may be considered are: the nature of the issues raised or likely to be raised in litigation; the amount that is or is likely to be in controversy; the nexus of the information to issues that may be involved in the litigation; the costs to preserve and potentially restore information; whether preservation would affect ongoing or future business activities; and whether there are other sources of such information, and other relevant factors.

8. Work with IT Personnel to determine appropriate method for preserving ESI.

9. Issue instructions with respect to future communications (e.g., limit use of e-mail; save relevant emails in particular folder; refrain from speaking or otherwise communicating with others concerning matter at issue).

10. Monitor compliance with Legal Preservation Notice through communications with Key Persons and the E-Discovery Response Team.

11. Issue periodic reminders that Legal Hold is still in effect.

12. Set review parameters and participate in ESI review process to the extent necessary to ensure appropriate

determinations are made regarding relevance, privilege, and other factors related to the duty to preserve ESI.

13. Manage any necessary production of ESI and other records in consultation with IT Personnel, Records Management Officers, the Attorney General (if AAG assigned), and other appropriate parties.

B. Custodians/Key Persons

1. Comply with all directives of the E-Discovery Response Team.

2. Understand the basic operations of electronic storage systems and programs that you use.

3. Manage records and ESI according to applicable laws, regulations, policies, and retention schedules. *This includes limiting the amount of ESI that is stored on systems and devices that does not have a legal, operational, or historical value to the University.*

4. Notify Counsel of threats of legal action and other potential Triggering Events.

5. If he or she is a "Key Person" and receives a Legal Preservation Notice, he or she has a duty to preserve relevant information as instructed by the Notice, no matter where it may be located, *including personal accounts and devices*.

6. Provide Counsel and the E-Discovery Response Team with information on the potential sources, locations, nature of relevant ESI, and other records in his or her possession or control.

7. Do not delete, destroy, purge, overwrite, or otherwise modify existing relevant ESI (or newly created relevant ESI) subject to a Legal Preservation Notice even if it is a duplicate, draft or "personal."

8. Give IT Personnel or Counsel access to all relevant records and ESI in order that such information can be preserved and retrieved if needed.

C. IT Personnel

1. Educate Counsel and Custodians on basic operations of systems, devices, and programs under their control, including back-up, archiving, and automatic deletion functions or programs.

2. Monitor use of IT systems to ensure Custodians comply with applicable policies, including those related to records management. This includes assisting in the destruction of records, documents and data for which the retention period has expired. This may be accomplished through automated systems, where practicable, such as in the case of email.

3. Contract and work with capable, responsible vendors. This may include vendors responsible for e-discovery services.

   Assist Counsel in identifying potential ESI sources.

4. Work with Counsel and Key Persons to implement Legal Holds. This may include having direct responsibility over ESI collection and preservation activities, pursuant to the direction of Counsel.

5. Upon direct receipt of a Legal Preservation Notice, or at the instruction of Counsel, take steps to preserve relevant ESI. This may include using administrative controls to lock down or copy information on University accounts and devices with or without the knowledge of the user.

6. Work with Key Persons to ensure preservation of relevant data created after the receipt of a Legal Preservation Notice, if any. This may include disabling automatic deletion systems or creating mirrored accounts and backups.

7. Be prepared to help Counsel review, produce and explain relevant ESI during any related legal proceedings.

D. Records Management Officers

1. The RMO on each campus shall act as the primary E-Discovery liaison with Counsel, unless the President makes another designation.

2. Promote campus-wide compliance with records management policies and best practices.

3. At the direction of Counsel, communicate directly with Key Persons and serve as a custodian of preserved material.

V. Other Guidance & Procedures

A. All electronic storage systems, devices, and programs purchased or used by the University should be functionally capable of meeting the obligations described herein. Generally, this means that they should at least be capable of long-term retention of ESI. It is considered preferable if such systems, devices, and programs also allow for the easy archiving, searching and sorting of ESI.

B. *Failure by any University officer, employee or agent to adhere to these procedures may result in discipline and expose him or her to legal sanctions.*

C. All officers, employees, and agents of the University should familiarize themselves with potential Triggering Events and communicate the occurrence or suspected occurrence of such events to Counsel through appropriate channels.

D. The exact scope, parameters, and features of a Legal Hold should be customized to the circumstances of the Triggering Event.

E. Campus policies should allow for administrative access and control of all University systems, programs, and devices. These policies should make clear to all employees that they have no privacy interest in University records and ESI, regardless of where such data are stored.

F. All University officers, employees and agents should document the steps they take pursuant to this policy and provide such documentation to Counsel when requested.

G. Campuses should encourage broad awareness of this procedure, make compliance with this procedure a priority, and provide adequate resources for such purposes.

H. The Office of General Counsel and the campus E-Discovery Response Team will routinely provide guidance to University leadership and constituencies.

I. The University will at all times strive to coordinate its efforts with applicable third parties (vendors, unions, etc.) and the Attorney General's Office to meet its E-Discovery obligations.

J. Except as modified by Legal Hold, Custodians must follow the SUNY Records Retention Policy (Policy 6609)

and schedules and should eliminate unnecessary copies/drafts of records and other documents, and should delete unnecessary email on a routine basis, typically 90 (ninety) days after it is sent or received. In sum, *ESI that is not included in the SUNY Records Retention Schedules and does not otherwise have an ongoing legal, operational, or historical value to the University should not be retained and stored on University systems.*

K. Back-up systems at University campuses should generally be used for the purpose of disaster recovery only. Time frames and cycles of such systems should be gauged accordingly.

L. Each campus should use its own procedures to supplement these University-wide procedures in order to better fit the local environment and organizational structure. Supplemental procedures so created shall be subject to the approval of the Office of General Counsel.

M. Supervisors, human resources and IT Personnel are jointly responsible for managing records and ESI that are associated with a separated employee in accordance with University policies and procedures.

N. University officers, employees, and agents should generally conduct official activities using University accounts and devices. Conversely, University officers, employees, and agents should generally refrain from using University accounts and devices for personal activities. The University shall have a right to inspect and monitor all use of its accounts and devices regardless of whether the use is personal or official.

Forms

SUNY Sample Template Legal Preservation Notice

SUNY Sample Questionnaire/ Interview Outline to Prepare for E-Discovery

---

Related Procedures

SUNY Procedure, Information Security Guidelines, Procedure Document 6608

Related Policies

Introduction to the SUNY Records Retention and Disposition Schedule, Policy Document Number 6609 Appendices

SUNY Policy, Records Retention and Disposition, Policy Document No. 6609

Other Related Information

SUNY Email Retention Guidance

Records Retention and Disposition at SUNY Campuses Guidance

Authority

NY Education Law Article 8, § 350 et seq.

History

This procedure was sent out via a Memorandum to State-Operated Campus Presidents by William F. Howard, Senior Vice Chancellor and General Counsel, on April 9, 2014.

Appendices

There are no appendicies relevant to this procedure.