ESI Incident Response Procedures

Objectives

1. Understand which policies, procedures and laws apply to ESI incidents.
2. Identify the types of situations that require that employees follow ESI procedures.
3. Document roles, procedures, and documentation procedures for ESI incidents.

Table of Contents

A. Applicable Policies, Laws and Procedures
B. Situations That Require Special Procedures
C. Detailed Instructions for Specific Situations that require more detail
D. Roles, Responsibilities and Definitions
E. General Concepts and Cautions That Apply To All Cases

Originally developed by the CIS Electronically Stored Information Work Group: Cooley, Eileen; Dinneen, Frankie; MacMillan, Manny; Cicerchi, Renee; Scovill, Bryan; Brym, Petr and approved by USNH Legal Counsel 10/26/2007 and UNH CIO 5/7/2008. Recent changes are highlighted in yellow.
A. Applicable Policies, Laws and Procedures

   This policy prescribes security requirements that must be followed by all USNH IT providers and users of institutional data.
   This policy prescribes what is considered to be acceptable use and behavior of UNH’s IT clients.
5. Outlines the expectations that the University has for its community members.
6. Applicable Laws
   a. FERPA – requires protection of students’ confidential information
   b. HIPAA – requires protection of medical information
   c. NH State statute, RSA 359-C:20 (Notification of Security Breach Requirement)
7. Campus IT Security Policy – This policy prescribes security requirements that must be followed by UNH IT providers (currently CIS is referencing the Indiana University security policy as an interim solution until the new CIS IT Security Officer leads an effort to write a formal UNH IT Security Policy).
8. Request Forms and Procedures
   a. Request to Release Student Telephone Call Records
   b. Request for Access to Confidential or Password-Protected Information
   c. Court-Order Request for Access to Confidential and/or Password-Protected Information
9. Other laws, per instructions from USNH Legal Counsel
B. Situations That Require Special Procedures:

Note: This section contains a general description of the situations you may encounter, and a brief description of applicable policies and procedures that guide your response. Where more detailed procedural information is needed, additional information if provided in section C.

1. **USNH Legal Counsel Informs CIS that certain electronically stored information must be preserved.** These situations are not very common, but are rapidly increasing in frequency, and can result in very large amounts of effort. In addition, if not handled properly, these situations could result in destruction of data that may be legally required at a later time by a third party leading to serious legal consequences. Follow instructions from the Legal Counsel and complete the steps outlined in the details section below. Assume that this initial request will be followed by a written order to preserve the information, and may be followed by a legal compulsion (e.g., search warrant, subpoena, court order) to disclose the information to a third party. Before proceeding, clarify what should be preserved, how it should be preserved, whether impacted persons must be notified, whether the request exceeds reasonable levels of effort, where else and/or who else may be storing the requested information, how to protect and store the data to prevent destruction, and whether the preservation and storage of the data could be violating other policies. Identify procedures, policies and or processes that could put the data at risk. Examples of such processes include backup tape rotation, automatic clearing of log files, or scheduled data destruction services. Discuss these issues with USNH legal and request guidance.

2. **One member (other than UNH Police) of the UNH community requests access to another person’s e-mail, voicemail, disk or data content, or any other content that is not explicitly available for public access.** These cases are relatively frequent, and the original request often is not acted upon as originally requested because further clarification results in a better understanding or what is actually needed. The requesting party often requires a briefing on USNH and UNH policies and applicable laws, and the request may need to be modified to comply with those laws and policies. Do not provide access and do not disclose the requested information without seeking approval. Inform the requestor that a special procedure may have to be followed. Alert your supervisor or senior manager who is on duty. The supervisor will inform the Director of IT Security, UNH CIO and/or USNH Legal Counsel, as appropriate. See instructions on the attached “employee.pdf” form titled “Request for Access to Confidential and/or Password-Protected Information” for detailed instructions.

3. **You are presented with a legal compulsion requesting information.** The legal compulsion could be a subpoena, a search warrant, etc. You are expected to and should comply with a legal compulsion. However, in some cases may be worded in a way that they cannot be acted upon due to conflicts with applicable laws, policy or due to technical limitations. If the legal compulsion is presented to you by a University Police you should assume that it is valid and proceed as instructed in the legal compulsion. If the legal compulsion is presented by a person
other than a UNH Police Officer, you are not expected to be qualified to determine whether the legal compulsion is valid, and therefore you must seek advice before proceeding. Inform the requestor that a special procedure may have to be followed. If the language in the document does not prohibit you from doing so and the requestor does not prohibit you from doing so, alert your supervisor or senior manager who is on duty and secure instructions on how to proceed. If the requesting party is an officer of the law and insists on accessing the required information immediately, contact USNH Legal Counsel immediately for advice while the officer is with you. Remember that you are responsible for not disclosing information that you are prohibited from disclosing by law or policy. The officer may not be aware of the laws or policies that apply to your actions. Make it clear to the officer that you are not obstructing, and that it is important that applicable procedures are followed. See instructions further explanation in the detailed section.

4. UNH Police requests access to information without a legal compulsion. Unless an employee, student or member of the public has a legally protected privacy interest in the records, data, or information sought, you can and should provide full and complete access to the UNH Police, without requiring any form of legal compulsion (e.g., search warrant, subpoena, court order). Ask the UNH Police representative whether you may notify your supervisor about the request. If the answer is yes, notify your supervisor but do not delay providing access to the requested information. If the answer is no, then proceed without delay with providing access to the requested information. Examples of information in which an employee, student or member of the public has a legally protected privacy interest in the records, data, or information sought include, but are not limited to health information, student educational records, and personal financial account information. Examples of information that you may provide to UNH Police include, but are not limited to employee work schedules, contact information, security surveillance video, building card access records, electronic content stored on UNH file servers that does not require legal compulsion, service records and incident/case records. UNH Police will typically present a legal compulsion when accessing communication records such as electronic mail and voice mail, but if the UNH Police indicates that the information is required immediately for the purpose of protecting life and safety, provide the information immediately.

5. UNH Housing Resident student asks for their own UNH phone system call records. You may not disclose this information without first verifying details of the request and ensuring that the request is compatible with the USNH and UNH policies. UNH Housing students share the same telephone line and voice mail in their room. You may not provide call records or access to the voice mail without explicit written permission from all roommates. A student who is the only occupant of a residence hall room and the only user of the phone number in question may request a copy of their call records for billing resolution purposes. A student who is requesting records for harassment, bullying, or other such investigative purposes should be referred to
UNH Police. Follow instructions on the back of the attached form "Student.pdf" titled "Request to Release Student Telephone Call Records".

6. Former member of the UNH community requests access to their e-mail or voice mail that has been terminated. You may not provide access without specific approval. Refer this request to the sponsored accounts process. The sponsored accounts process and policy was recently updated and moved to an on-line service at https://remedy.unh.edu/Accounts/Sponsored/.

7. Anyone, other than UNH Police, requests information about another individual, such as their account usage information, passwords, etc. Do not provide access and do not disclose the requested information. Inform the requestor that a special procedure may have to be followed. Notify your supervisor. Such requests may require a legal order, VP approval, and/or notification of the person(s) affected. Specific language in the USNH IT Security Policy applies to this situation, and your response must be compatible with that policy. USNH Policy prohibits sharing of passwords. When providing authorized access to password protected information, rather than sharing passwords, accomplish doing so by temporarily changing appropriate access privileges or providing copies of the requested information. Refer this request to your supervisor for oversight.

8. If the situation you are handling does not fit any of the above scenarios or you have any doubts, seek advice from your supervisor, Director of IT Security, UNH CIO, and/or USNH Legal Counsel. If you are instructed that you may not disclose information about the situation to anyone but you do not know how to proceed, you may contact USNH Legal Counsel for further guidance.

C. Detailed Instructions for Specific Situations

USNH Legal Counsel informs CIS that certain information may or will be required for a legal case and must be preserved.
1. Notification includes at minimum a live contact by telephone or in person to alert CIS to this case, followed by an appropriate written request with clarification details. The initial notification is provided to the primary ESI contact; if the primary ESI contact is not reachable, USNH Legal Counsel will notify the ESI contact backup through the UNH CIO office. All reasonable effort must be made, starting from the time of the initial notification, to protect the pertinent information from destruction.

2. Primary ESI contact notifies ESI members and UNH CIO about this request. The purpose of this communication is to make the ESI member aware of the situation, avoid duplication of effort and/or overlooking steps that need to be completed. Also, ESI members can help identify potential sources where the information in question may be stored.

3. Primary ESI contact works with the ESI work group, if necessary, to determine who must be involved in meeting this request, and to identify a coordinator for this case.

4. The coordinator works with USNH Legal Counsel, data stewards and technical staff to clarify details of what is requested.

5. The coordinator determines in cooperation with USNH Legal Counsel what exactly must be preserved, how it will be preserved, how it will be stored, how long it will be stored, what resources are needed, when the information can/will be provided, and any notifications that must be made. The coordinator and USNH Legal Counsel will also determine if any of the proposed response exceeds reasonable levels of effort or cost, and in such cases they will propose modification of the request to the requesting party.

6. The coordinator assumes responsibility for managing the specific response outlined in #5 above, ensuring that timely progress is made and to document progress. The coordinator will keep USNH Legal Counsel informed about progress and any concerns. Records about progress of this case will be maintained in a protected area of Remedy to which only ESI members will have access. Coordinator will notify UNH CIO office within one week of completion of the case and file with that office any paper documents that require long-term storage (ex. Original subpoena, signed documents, etc.). ESI members will not store, long-term, any paper documentation on such cases in their office areas.

7. Upon successful and confirmed transfer of the requested information to the requesting party, the coordinator will confirm with USNH Legal Counsel that we can return to standard data retention and data destruction procedures that involve destruction of the data in question.

8. Access to the actual information in question will be limited to those persons who must work with it to provide it as requested, and provided only to those specified by USNH Legal Counsel. Information about the case will be shared with others only on a need-to-know basis, and in compliance with any specific instructions from USNH Legal Counsel.

You are presented with a legal compulsion requesting information. The legal compulsion could be a subpoena, a search warrant, etc.
1. If the document appears to be an original search warrant issued by the United States District Court for the District of New Hampshire, the New Hampshire Superior Court or the New Hampshire District Court is presented to you by the UNH Police Department, you may assume that the document is valid. If the document is presented by any other person or organization or represents itself to be anything other than a search warrant (e.g., subpoena, request for production of documents, etc), you must obtain clarification from USNH Legal Counsel about the document’s authenticity and legal status before proceeding.

2. In all cases, begin to assemble the requested information and inform your supervisor, the USNH Legal Counsel, the UNH CIO’s office and your supervisor that you received a legal compulsion (document) that is requiring you to disclose certain information, specify what are your intended steps to respond to it, and ask whether you are approved to continue responding to the legal document. You should inform the officer serving the request: a) UNH will comply with state and federal law, b) you do not have authority to bind the University to a legal position regarding a response to the demand for production of ESI, c) UNH handles information that is subject to a variety of state and federal laws, and therefore we have policies that help us be sure that we comply with applicable laws when ESI is demanded or requested and d) you will move expeditiously both to gather the ESI sought under the request or order and to clarify our authority to respond. Please avoid statements to law enforcement officers suggesting that UNH policies in any way supersede state or federal criminal law.

3. If the legal compulsion prohibits you from notifying anyone that you were served the legal document, contact USNH Legal Counsel for advice.

4. Review the legal compulsion (document) and determine whether the documented request is clear, whether the data requested is available, whether the data is obtainable with a reasonable amount of effort and cost, and whether others must be involved in securing the requested data.

5. Determine whether notification of the person(s) to whom the requested information pertains is required. If yes, and the legal compulsion does not prohibit doing so, work with the office of Student Affairs, Human Resources, or other applicable administrative offices to complete the appropriate notification process. Please bear in mind that in some instances a court will order us not to inform the “target” of the request for ESI or notification of the target is not required by state law, federal law or UNH policies.

6. Depending on the answer from USNH Legal Counsel, your supervisor and the UNH CIO’s office, inform the requesting party whether you will be able to respond to the legal document in the time frame called for in the document, and whether you will be able to provide the information as requested.

7. Negotiate with the requesting party the format and mechanism that will be used to provide the requested data. If the requested data is not obtainable as requested, negotiate with the requesting party a reasonable alternative. For example, if the request is for any and all e-mail
messages for the last ten years, and backup of e-mail is only available for the past one year, negotiate with the requesting party an updated written request for e-mail for the past one year.

8. Gather the requested information and provide it to the requesting party in a secure and documented manner. Verify successful transfer of the data to the requesting party and that they are able to read the information while you can still repeat the gathering and packaging of the information if the transfer is not successful.

9. Notify USNH Legal Counsel, your supervisor and the Director of IT Security (or UNH CIO office) within one week of completion of the work and file with that office any paper documents that require long-term storage (ex. Original subpoena, signed documents, etc.). Do not store, long-term, any paper documentation on such cases in their office areas.

D. Roles, Responsibilities and Definitions
ESI Work Group (Electronically Stored Information work group) – This work group is charged "To work with USNH legal staff to maintain an interim protocol for responding to legal information requests under the new ESI discovery rules. This group is not being charged to develop policy for data retention. It will focus on operational plans for response to legal requests." The Director of IT Security chairs this working group and requests work sessions when necessary.

USNH Legal Counsel – Provides legal interpretation and advice to UNH employees (this language will be updated by USNH Legal Counsel)

UNH CIS IT Security Committee - Guides and supports a deliberate and coordinated effort to establish reasonable security standards and policies, to identify IT security concerns, and to guide CIS in the development of strategies to protect the institution’s IT infrastructure, content, and clients

Data Stewards – Provide guidance and have authority over access to and disclosure about institutional information such as, but not limited to Human Resources data, Financial Information, and Student Information.

System and/or Database Administrators – Provide technical expertise for managing and accessing institutional information under the guidance and authority of data stewards.

Institutional Data – Information stored by and in institutional resources, such as HR, Finance, and Student information stored on UNH file servers, paper documents, or backup media. (this definition needs to be expanded)

Legal Compulsion - Search warrant, subpoena, and court order.

UNH Community Member – UNH faculty, staff and students. It may include certain visitors, volunteers, service providers and clients.

USNH Community Member - Faculty, staff and students from any of the USNH institutions including UNH, UNHM, GSC, PSU and KSC. It may include certain visitors, volunteers, service providers and clients.

IT (service) Provider – Member of the central computing service department such as CIS and/or member of a college, RCM unit or department who provides information technology services (includes academic technology liaisons, for example).
E. General Concepts and Cautions that apply to all cases:

- You never have to do this alone - Be aware that in some cases you may not be able to notify anyone else that you have been asked to provide information. In those cases invite the requesting party to call UNH Legal Counsel directly. Normally you should notify your supervisor in order to establish appropriate oversight for your action, however, if you are not allowed to notify your supervisor, notify USNH Legal Counsel. Please note details above referencing requests from UNH Police.

- Need to know basis - When asked to provide information to others, provide only the information you know explicitly that you are authorized to provide. When in doubt, contact your supervisor. Disclose only the information that is required for the situation at hand. Give only the information needed so the next proper step can happen. Don’t broadcast and don’t talk with colleagues about the case. Do not generate written notes, e-mails, voice messages or other forms of communication that may be accessed by unintended persons.

- Documentation – Verify what documentation is required for each case. Do not store information on your personal computer. Protect all information from others seeing or accessing it. Remember that all written documentation is subject to review by courts. Ask what policies apply to long-term storage and destruction of any documentation for the case in question.

- Role of Data Steward - If you are being asked for data for which you are not the authorized data steward, refer the case to the data steward for guidance.²

---

² This is the last page of the approved core document.
Frequently Asked Questions

1.) As an IT employee, am I expected to look for illegal content on client machines when I work on them?
   i. Proposed Answer – You are not expected pro-actively look for such content.
   ii. Proposed Answer – Policy prohibits viewing client content unless doing so is an integral part of performing an approved service.

2.) What content should be reported to UNH Police if I come across the content while performing approved service?

3.) What should I do if I am presented a legal compulsion or request to disclose information to any other police agency than UNH Police?
   i. Proposed Answer – Ask the requesting party to work through UNH Police.

4.) Will UNH Police present a written legal compulsion to obtain building access information?
   i. Proposed Answer – UNH Police will bring a warrant when seeking building access information for student residence halls.
   ii. Proposed Answer – UNH Police will typically not bring any legal compulsion when seeking building access information for administrative buildings.

---

3 These frequently asked questions are not part of the approved core document. They will be incorporated into the next revision of the document and approval process.