ESI Incident Response Procedures

Developed by UNH CIS in coordination with USNH Legal and adapted for KSC. Approved, KSC CIO, 8-11-2008

Table of Contents

A. Applicable Policies, Laws and Procedures

1. Electronically Stored Information Rules – [http://www.uscourts.gov/ttb/11-06/electronically/index.html] and [http://www.uscourts.gov/rules/Reports/ST09-2006.pdf.]
2. USNH IT Security Policy This policy prescribes security requirements that must be followed by all USNH IT providers and users of institutional data.
3. KSC Data Access Policy
4. CNUP (Computer & Network Use Policy)
5. Students Rights & Responsibilities
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 KSC IT providers
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:**

1. **USNH Legal Counsel informs the IT Group that certain electronically stored information must be preserved**. ***Initial notification is provided to the CIO Office.***

   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. CIO will follow instructions from the Legal Counsel and inform appropriate staff to 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 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. **CIO will discuss these issues with ITG Security Manager and request guidance from USNH legal.**

2. **One member of the KSC 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. The requesting party often requires a briefing on USNH and KSC 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 the ITG Security Manager. The ITG Security Manager will inform 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 document requesting information. The legal document could be a subpoena, a search warrant, etc.** These requests are not uncommon, and in some cases may be worded in a way that they cannot be acted upon due to conflicts with applicable laws or policy. You are not expected to be qualified to determine whether the court order 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, alert the ITG Security Manager 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 below in the detailed section.

4. **KSC Residential Life student asks for their own KSC 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 IT security policy. KSC Residential Life students share the same physical telephone line in their room. However, students have individual personal voicemail boxes. You may not provide call records 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 KSC Campus Safety. Follow instructions on the back of the form titled "Request to Release Student Telephone Call Records".

5. **KSC employee requests phone system call records of another employee.**

   You may not disclose this information without first verifying details of the request and ensuring that the request is compatible with the USNH IT security policy. Follow instructions on the back of the form titled "Request for Access to Confidential and/or Password-Protected Information".

6. **Former member of the KSC community requests access to their e-mail or voice mail that has been terminated.**

   There is no data available. Email and voicemail records are deleted upon account deactivation.

7. **Anyone 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. 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. Refer this request to ITG Security Manager 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 ITG Security Manager and/or CIO.**

C. Detailed Instructions for Specific Situations

USNH Legal Counsel informs IT Group 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 IT Group to this case, followed by an appropriate written request with clarification details. The initial notification is provided to the CIO Office. All reasonable effort must be made, starting from the time of the initial notification, to protect the pertinent information from destruction.
2. CIO will notify ITG Security Manager. The purpose of this communication is to make the Security Manager aware of the situation, avoid duplication of effort and/or overlooking steps that need to be completed. Also, the security manager can help identify potential sources where the information in question may be stored.
3. IT Security Manager will assume coordinator for the case.
4. The coordinator works with USNH Legal Counsel, data custodians 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 above, ensuring that timely progress is made and to document progress. The coordinator will keep USNH Legal Counsel and campus CIO informed about progress and any concerns. Records about progress of this case will be maintained in a secure tracking mechanism in which only appropriate staff will have access. Coordinator will notify 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.). Any documentation on such cases will not be stored long term in staff 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 KSC standard data retention and data destruction procedures as dictated by institutional Data Access Policy.
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 document requesting information. The legal document could be a subpoena, a search warrant, etc.

1. If the legal document is presented to you by the City of Keene, you may assume that the document is valid. If it is presented by any other person or organization, you must seek clarification from USNH Legal Counsel about whether the document is valid before proceeding.
2. Inform ITG Security Manager and your supervisor that you received a legal 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.
3. If the legal document prohibits you from notifying anyone that you were served the legal document, contact USNH Legal Counsel for advice.
4. Work with ITG Security Manager to review the 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.

ITG Security Manager coordinates and communicates the following steps.

1. Determine whether notification of the person(s) to whom the requested information pertains to is required. If yes, ITG Security Manager and/or CIO will work with the office of Student Affairs, Human Resources, or other applicable administrative offices to complete the appropriate notification process.
2. Depending on the answer from USNH Legal Counsel, the ITG Security Manager and/or CIO will 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.
3. 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.
4. 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.
5. Notify the CIO's 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. CIO will notify USNH Legal Counsel.

D. Roles, Responsibilities and Definitions

USNH Legal Counsel – Provides legal interpretation and advice to KSC employees

KSC Security Manager - Guides and supports a deliberate and coordinated effort to establish reasonable security standards and policies, to identify IT security concerns, and to guide IT Group in the development of strategies to protect the institution's IT infrastructure, content, and clients

Data Custodians – 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. If you are being asked for data for which you are not authorized to provide, refer the case to the data proprietor for guidance

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

Institutional Data – Information such as HR, Finance, and Student stored **on** KSC file servers or **off site** file servers (ASP), paper documents, or backup media.

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

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

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 USNH Legal Counsel directly. Normally you should notify the ITG Security Manager in order to establish appropriate oversight for your action.
- 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 the ITG Security Manager. 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.