



**Request for Access to Confidential and/or Password-Protected Information**

When completing this form, please use only blue or black ink and complete all fields. See reverse for instructions.  
8/11/2008

**To: Information Technology Group**

**Requestor:** \_\_\_\_\_

**Requestor Credentials:** \_\_\_\_\_

**Request Approved By:** \_\_\_\_\_

**Detailed Description of Request:**

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Requestor's Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_ **ID Ver.\*** \_\_\_\_\_

**OFFICE USE ONLY**

Form Received By:	Signature: _____	Date: _____
Records Released By:	Signature: _____	Date: _____
Records Received By:	Signature: _____	Date: _____

Form Instructions for Requestor:

- 1 **Applicable Situation(s)** — KSC community member requesting to access another member's telephone call records, electronic mail and/or computer storage media content.
- 2 **Requestor Credentials** — Proper credentials are required when submitting this form. Supervisors or an authorized manager/director is qualified to submit this request.
- 3 **Request Approved By** — Proper authorization from the appropriate Principal Administrator is required when submitting this form.
- 4 **Detailed Description of Request** — Required Information:
  - 4.1 Date of the request
  - 4.2 Phone number(s) in question (when applicable)
  - 4.3 Information/storage media in question
  - 4.4 Date(s) in question
  - 4.5 Room(s)/location(s) of the phone number(s)
  - 4.6 To whom the information is being released
  - 4.7 Names and signature of any individuals with shared access to the information being requested

Example:

"I am requesting access to electronic mail for employee Jane Doe for records dating May 1, 2008. I am Jane Doe's direct supervisor and have authorized my credentials on this form. No other employees share this information, and I have obtained proper Principal Administrator authorization."

- 5 **Submit** completed form to **HelpDesk, Elliot Hall, 2<sup>nd</sup> floor**

**Instructions for HelpDesk Staff:**

- 1 HD staff receiving this form must confirm the identity of each individual signature via photo identification and initial where appropriate next to each signature.
- 2 Alert IT Group Security Manager of the submitted request and make arrangements to securely deliver the document to the receiving manager.
- 3 HD staff securely transfers the original request document(s) to ITG Security Manager.
- 4 **CAUTION:** If at any point the case appears to deviate from the process described above, IT Group Security Manager consults CIO as appropriate.

**Instructions for IT Group Security Manager:**

- 1 Security Manager receives request form from HelpDesk staff and verifies the form was filled out completely, and notifies CIO as appropriate to document the process and IT Group's intention to release the information. The notification documents the situation, but if sent via electronic mail, does not contain any employee names and/or phone numbers unless specifically requested.
- 2 IT Group staff generates the requested call records and/or arranges for access to password-protected information and delivers information in a sealed envelope to ITG Security Manager for safe storage until authorized individual receives records.
- 3 If no questions remain about whether the appropriate process was followed, and/or no concerns are raised by CIO or USNH Legal Counsel, ITG Security Manager notifies the authorized employee that the information is ready to be picked up and makes arrangements for the pickup.
- 4 Upon successful delivery of the record(s) to the authorized employee, ITG Security Manager documents the transfer on the request form and the receiving employee prints name and signs the form to confirm receipt of the records. **All documentation including original request documents will be delivered to CIO office where they will be stored in locked storage.**
- 5 **CAUTION:** If at any point the case appears to deviate from the process described above, ITG Security Manager consults CIO as appropriate.