Requesting Access to a Covered Individual’s Information Resources

Subject: Requesting Access to a Covered Individual’s Information Resources
Date: 7/1/2017
Authorized by: Sara Saathoff, Assistant Dean and Executive Director
Biological Sciences Division (BSD) Human Resources

Purpose:

The purpose of this policy is to establish guidelines for requesting, authorizing and handling electronic information (e.g., emails, computer files, etc.) of a covered individual when s/he transfers or ends his/her assignment with the BSD, or is out for an extended leave, to ensure a smooth transition and continuity of services. This protects the organization's physical property, maintains an operating knowledge base, and ensures compliance and security regarding University, Divisional, UCM and Departmental IT resources and assets.

Scope:

This policy applies to staff employees and students of the Biological Sciences Division (BSD), individuals who fall within the definition of "Workforce" of the organization, and third parties with access to the organizations’ Information Systems and/or the organization's Information Assets ("Covered Individuals").

Policy:

The Biological Sciences Division (BSD) expects that Department Head/Unit Leaders take the precautionary measures outlined in the General Guidelines in order to limit requests to a covered individual’s information resources.

Access to a covered individual’s information resources requires approval from the departmental Human Resources Professional (HRP) and University Legal Counsel in advance of submitting the request for access to CBIS, ITS and/or departmental IT custodian. Requests to the departmental HRP and University Counsel will be assessed using framework and standards set forth in the University’s Acceptable Use Policy.

Any review, whether limited to e-mail and e-mail attachments, or computer files (electronic files) pursuant to authorized access, should be limited to the minimum necessary review in order to resolve the situation. Access to the former covered individual's information resources normally will be limited to ninety (90) days or less.

Note: The above policy and following guidelines supplement responsibilities set forth in other University policies including, but not limited to, the University's personnel, financial and administrative policies, the Employee Handbook, the Student Manual, and any other departmental handbook, manual, policy, or procedure.

Definitions:

Covered Individual: Employees and students of the BSD, individuals who fall within the definition of "Workforce" of the BSD, and third parties with access to Information Systems and/or the Information Assets
**Department and Unit Leader:** Leaders within the Organizations (e.g. Department Chairs, Section Chiefs, Executive Directors, Directors, Managers, Supervisors, etc.)

**Designated Custodian:** Person being granted access

**E-mail Attachment:** A file sent along with an e-mail message

**E-mail:** The electronic transmission of messages from sender to recipient

**Endpoint:** Any desktop or laptop computer (e.g., Windows, Mac, and Linux/Unix), Mobile Device or other portable device used to access Organizational Information Resources from any local or remote location or access any Organizational Information System either owned by the Organization or by an individual and used for Organizational purposes

**Information Assets:** Any piece or collection of information

**Information Resource:** Servers, endpoints, storage, network and storage switches, firewalls, physical racks containing these, and related software that are components of Information Systems

**Information resources:** All electronic equipment (e.g., computers, laptops, tablets, cellphones, and other electronic devices) and information generated, used, or stored by any user, including documents, files, e-mails and attachments, research data, voice mails, text messages, and associated metadata

**Information System:** Server based software that resides on a single Server or multiple Servers and is used for business purposes. "Application" or "Information System" is synonymous with System" (e.g., a database server, web server or other application server)

**IT Custodians:** Employees who are technical administrators of the Information Systems and Information Assets used by the organization

**Personal Share or User Folder:** An electronic folder located on the University of Chicago (UC), Biological Sciences Division (BSD) and/or University of Chicago Medical Center (UCM) network that has been established for a specific end user where access is limited to that user

**Workforce:** Employees and students of the BSD, individuals who fall within the definition of "Workforce" of the BSD, and third parties with access to Information Systems and/or the Information Assets

---

**General Guidelines:**

When a covered individual joins the organization, the manager/immediate supervisor should ensure to:

- Establish BSD e-mail accounts and file shares for all users, and direct users to utilize these shared information technology resources to store work that is valuable to the ongoing operation of the department.

- Establish the expectation that personal use of UC, BSD and/or UCM accounts should be incidental and that individual accounts and their contents are the property of the University.
When a covered user ends his/her relationship with the Biological Sciences Division (BSD) Managers/Supervisors are encouraged to perform the following step to ensure a smooth transition of all business-related electronic information stored on the covered user’s UC, BSD and/or UCM information technology resources:

- Review information technology resources prior to separation.
- Prior to a covered individual’s separation, have the user review their individual information technology resources to move messages and files of ongoing value to a common departmental account or storage area, and delete or move personal information to other non-BSD information technology resources.
- Remind the separating individual that all information technology resources are property of the University.
- Set an “auto-reply” message on e-mail accounts and a voice-mail message that directs people to alternative sources for assistance.

In cases where the above general guidelines are not followed, or other extenuating circumstances exist, the following Authorization Procedure must be followed.

**Authorization Procedure:**

In cases where the General Guidelines were not adhered to, or other extenuating circumstances exist, the Information Resource Access Request form and Confidentiality Agreement must be completed by the manager or immediate supervisor and approved by departmental Human Resources Professional (HRP) and University Legal Counsel before access may be obtained to a former covered individual’s information resources.

The procedure for obtaining authorization is as follows:

- The former covered individual’s manager or immediate supervisor must complete the Information Resource Access Request form, and submit it to their departmental HRP for review. A manager may request access to the covered individual’s e-mail and attachments, and/or computer files for him/herself or another individual.
- If the departmental HRP is supportive of the request, s/he will sign in approval and forward the approved request to University Legal Counsel for review and authorization.
- Upon receiving University Legal Counsel’s authorization to move forward with the request, the departmental HRP will coordinate access to the former covered individual’s information resources with CBIS, ITS or departmental IT custodian.
- CBIS, ITS and/or departmental IT custodian will oversee the process of accessing UC, BSD and/or UCM information resources of the covered individual.
- CBIS, ITS and/or departmental IT custodian will ensure that the designated custodian’s access is removed as outlined in the approved request.

There are circumstances that warrant Divisional HR and/or IT involvement; these will be handled on a case-by-case basis.

**Expectations for IT Custodians:**

IT Custodians must make sure that appropriate approvals have been obtained before accessing a current or former covered individual’s email and attachments, computer files or other data on UC, BSD and/or UCM information resources. They should not copy, send, or otherwise share the files or data with anyone unless they have received written authorization to do so.

IT Custodians must remove the designated custodian’s access as outlined in the approved request.

**Expectations for Designated Custodian:**
While the BSD makes information resources available to its users for the primary use of education, research, clinical, and administrative activities, it recognizes that users may occasionally use BSD information resources, especially e-mail accounts, for incidental non-business related use. Thus, it is reasonable to expect that the BSD will provide protection for the covered individual’s personal information as long as it does not violate any local, state or federal laws and regulations. If it is determined that information is of a personal nature or is non-business related, the user should cease looking at it and refrain from sharing it with others.

While performing these duties, if any user comes across material that they reasonably believe to be of a criminal nature (e.g., child pornography, criminal conspiracy, etc.), they must stop the search, secure the PC or other resource, and immediately contact University Legal Counsel.

**Related Policies:**

- U601 – Treatment of Confidential Information
- U1007 – Responding to External Request for Information
- U703 – Progressive Corrective Action
- U705 – Employee Access to Personnel Records
- IT Services Account Closure Policies and Procedures
- The University of Chicago Policy on Information Technology Use and Access and FAQs
- BSD Cyber Security Policies