

**Title:** Guidelines for Handling a Former Employee's Personal Computer and Associated Files  
**Review Date:** November 22, 2011  
**Issuing Authority:** Chief Information Security Officer

---

When an employee ends his/her employment relationship with the University, there is sometimes a need to access business-related information stored on the former employee's University computing resources. According to University policies, access to computing resources is strictly prohibited unless a person is the account holder or has permission from the account holder. Any exceptions to this policy must be approved by The VP for Computer and Information Services following receipt of advice and consent of University Counsel and the Office of the President. To facilitate the needs of a department to continue with normal business operations, all supervisors are advised to obtain such permission from the employee prior to his/her leaving Temple employment. To assist in this process, the Human Resources Termination Check List contains a release form which the exiting employee can sign to release his or her files to the supervisor.

These guidelines supplement the termination process and guide the supervisor in determining what may be done with a former employee's University computing resources. These guidelines also provide direction to Computer Services as to what it may do with a former employee's University computing resources, whether or not a written release is obtained.

#### **Department Heads:**

1. When an employee gives notice of resignation, the department head should inform the employee that the employee must provide access to all University data stored on any University computing resource used or controlled by the employee. The department head should ask the employee to remove any personal files from his/her PC, network drives and email account, and should remind the employee that Temple University's confidential and proprietary data must remain with Temple and that all work-related material is the property of Temple University.
2. The department head should use the Termination Checklist at (<http://Voyager.adminsvc.temple.edu/EmployeeForms/Forms/HumanResources/TerminationCheckList.doc>) and make sure that the employee signs the release prior to the employee leaving the University's premises. The release allows the supervisor to access the employee's business-related email and files on the employee's PC and network drives in accordance with Section 16.7 of the Temple University Employee Manual.
3. The department head should retain the signed release form in the department's files and forward a copy to Human Resources.
4. If the employee has already been terminated and has left the workplace without signing a release, the department head promptly should attempt to contact the employee to obtain the required release. If the employee declines to sign a release, an Authorization Form (See Authorization Procedure below) will be required before the department head may access the employee's computer files or e-mail messages. Upon approval of the Authorization Form, the department head may schedule an appointment with Computer

- Services (call 1-8000) to assist in accessing the employee's files and, if necessary, transfer relevant business-related folders, files and other data to a CD or DVD. Note that files or other data that are reasonably deemed to be of a personal nature should not be copied or transferred, except in extenuating circumstances.
5. If the employee's emails are needed, the department head should contact Computer Services to request access to the employee's business-related email messages. (Access to an employee's emails requires a signed release or an approved Authorization Form).
  6. Departmental access to a former employee's data has time limitations. A terminated employee's email messages ordinarily may only be accessed for 30 days.

### **Computer Services:**

1. Computer services personnel should make sure that appropriate approvals have been obtained before accessing a current or former employee's files or other data on University computing resources. Do not copy, send, or otherwise share the files or data with anyone unless you have received the appropriate signed release or approved Variance Form.
2. If you determine that information is of a personal nature or is non-business related, you should cease looking at it and refrain from sharing it with others, except as set forth below.
3. While performing your duties, if you come across material that you reasonably believe to be of a criminal nature (e.g., child pornography, criminal conspiracy, etc.), stop your search, secure the PC or other resource, and immediately contact the Office of the CISO.
4. All criminal investigations involving University computing resources must be coordinated with the Office of the CISO who will work with Campus Police and/or external law enforcement to ensure that chain of custody and rules for evidence are maintained.
5. Personal Computers of former employees should be "wiped" and re-imaged prior to reissue.

### **Office of the CISO**

1. Maintain guidelines on the process of accessing a terminated employee's personal computer and associated files.
2. Ensure that Computer Services receives and files approvals prior to authorizing access to the former employee's personal computer and associated files.
3. Maintain the Authorization Procedure.
4. Work with Campus Police and external law enforcement agencies on all investigations involving computing resources.

**VP for Computer and Information Services, University Counsel and Office of the President**

1. Approval by the VP for Computer and Information Services, University Counsel and the Office of the President is required for access to all University computing resources for which a release has not been obtained and filed. These approvals should be obtained through the Authorization Procedure.

**Authorization Procedure**

1. Following an unsuccessful attempt to obtain a release, a Authorization Form (see below) must be completed and approved before access may be obtained to a former employee's University computing resources.
2. The department head or managing supervisor of the former employee must complete a Authorization Form, and the department head must sign it.
3. The Authorization Form is sent to the Office of the CISO, 705 Conwell Hall. It may be faxed to 215-204-5656.
4. The CISO will review and make recommendations to the VP for Computer and Information Services.
5. The VP for Computer and Information Services may authorize access following receipt of advice and consent of University Counsel and the Office of the President.
6. The Office of the CISO will oversee the process of accessing University computing resources of the former employee.

**Authorization Procedure  
For  
Accessing a Former Employee's Computing Resources**

Date of Request: \_\_\_\_\_

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

Employee's Name: \_\_\_\_\_

Employee's TUID \_\_\_\_\_

Was there an attempt to obtain a release (yes/no)? \_\_\_\_\_

Reason for not receiving a release:

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

Do you know specifically which files are needed (yes/no)? \_\_\_\_\_

If yes, please list needed files:

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

Department Head \_\_\_\_\_

Chief Information Security Officer \_\_\_\_\_

VP for Computer and Information Services \_\_\_\_\_