

## **Office of Research and Graduate Studies Data Handling Procedures**

Due to the nature of the materials handled by the Office of Research and Graduate Studies (ORGS), this office handles and stores confidential information relative to students, staff, and faculty. Accordingly, all personnel must comply with the TTU Data Security Policy (<http://www.tntech.edu/its/policies/DataSecurity.htm>) and must sign the appropriate university confidentiality statement (website). Specific office procedures dealing with data security are as follows:

### **General**

1. Keys are distributed only to TTU ORGS Office employees. Regular employees must obtain keys through university key issuance procedures. No keys will be assigned or loaned to part-time, temporary employees or TTU students. No unauthorized copying or sharing of keys is permitted.
2. Neither the office nor the storeroom should ever be left unattended unless they are locked.
3. ORGS personnel should not use their keys to allow access to the ORGS office or storeroom to an unauthorized individual.
4. The filing cabinets should be locked when the office is closed.
5. When sharing Level III information verbally, either over the phone or in person, ORGS personnel should be aware of any non-ORGS personnel present and take care to limit the information that can be overheard.
6. If Level III or other sensitive information is not being actively used by ORGS personnel, it should not be left out in a manner that a casual observer could view it.

### **Sending Information**

1. When sending Level III information via e-mail, for now it should be password protected, and it should be encrypted once a method to do so is approved by ITS.
2. Sending Level I or II information via e-mail does not require password protection or encryption unless the ORGS employee sending it determines that the information is of such a sensitive nature that it needs extra protection.
3. All e-mails should have a confidentiality statement included as a default at the bottom of the page. It should be similar to the one included in the confidentiality statement section below.
4. When snail mailing or hand delivering Level III information, the campus mail envelope should be addressed to the specific person it is going to, and a "confidential" sticker should be placed on the envelope.

5. When snail mailing, the Level III information itself should be stamped “confidential” or a statement such as the one in the confidentiality statement section below should be attached to the front of the information.
6. When sending Level III information via fax, a fax cover sheet with the confidentiality statement similar to that in the confidentiality statement section below should be used. The first page of the Level III information being faxed should be stamped “confidential.”
7. When snail mailing, hand delivering, or faxing Level I or II information, no special measures are required, but ORGS personnel should use their own discretion as to any additional measures necessary if the information is very sensitive.

### **Receiving Information**

1. When any information is received in the ORGS office, it should not be shared or distributed prior to evaluating the appropriateness of doing so.
2. Office workstations must have the screen-saver password feature enabled. When non-ORGS personnel are present, sensitive information, regardless of level, should be minimized or the screen-saver feature should be allowed to come on.

### **Control of Electronically Stored Information**

1. Level III information stored on workstations and laptops must be password protected (for now) and encrypted (once the method to encrypt has been approved).
2. No Level III information should be stored on any flash drive other than the Ironkey or other ITS approved flash drive.
3. No Level III information should be kept on floppies or CDs.
4. Passwords to any electronic storage medium should be kept in the locking file cabinet. Passwords should never be left out.
5. Passwords to electronic mediums should not be shared with non-ORGS personnel unless necessary for ITS, ORGS staff from other universities, or state audit personnel to perform required tasks.

## **Physical Location and Controls of Data Storage Devices**

1. The file cabinets with passwords and transcripts should be kept locked unless being actively used.
2. The key to the ORGS storage room should not be shared with anyone other than ORGS personnel.
3. When not in use, the ORGS laptop should be kept in one of the file cabinets that are always kept locked in the main office.
4. Floppies and CDs require no special storage within the office as they should not contain any Level III information.

## **Disposal of Data**

1. Level I, II and III data must be shredded either by or in the presence of ORGS personnel.
2. If a computer is being surplus or transferred to another office, ITS personnel must perform the appropriate level wipe of the hard drive.
3. In all cases, working papers must be kept for a minimum of 5 years. If another audit has not been done in the area after the 5 years, or it is a unique investigation, then ORGS personnel will use their discretion in determining how long to keep the working papers, from 5 years up to indefinitely. The Office of Research must maintain externally funded project files for 3 years after the end date of the project, except if projects have resulted in invention disclosure.
4. The most recent working papers should be kept in the main office. When they are no longer useful or space does not permit keeping them in the main office, they should be transferred to the storage room.
5. All other data should be destroyed as time permits and space issues arise, but never before the minimum time specified in TBR Guideline G-070.

## **Releasing Information**

1. No information collected/created in ORGS can be released to the general public except published reports that have been accepted by the TBR. Only full-time employees of ORGS can release information to a requestor.
2. If a Tennessee resident requests to view a published report, they can do so. Any copies or arrangements to view the reports must be accommodated within seven days of the request. A Tennessee driver's license should be examined to determine residency.
3. If the requestor wants a copy, determine the number of pages to be copied and multiply that times 15 cents. If the number of copies needing to be made is such that over an hour is needed to make the copies, then a labor charge should be added to the copy cost. The labor cost should be calculated as outlined in TBR policy 4:07:10:00. After the total cost has been determined, the individual making the request should go to the Business Office window

and pay the charges. Upon presentation of the receipt in ORGS, ORGS will make a copy of the receipt and release the copies to the requestor.

## Definitions

**Level I data** — Access to Level I institutional data may be granted to any requester, or it is published with no restrictions. Public data is not considered sensitive. The integrity of “Public” data should be protected, and the appropriate department or unit must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should Level I data not be available is typically low, (inconvenient but not debilitating). Examples of Level I “Public” data include published “white pages” directory information, maps, departmental websites, and academic course descriptions.

**Level II data** — Access to Level II institutional data must be requested from, and authorized by, the department or unit who is responsible for the data. Access to internal data may be authorized to individuals based on job classification or responsibilities (“role-based” access), and may also be limited by one’s employing unit or affiliation. Non-Public or Internal data is moderately sensitive in nature. Often, Level II data is used for making decisions, and therefore it’s important this information remain timely and accurate. The risk for negative impact on the institution should this information not be available when needed is typically moderate. Examples of Level II “Non-Public/Internal” institutional data include project information, official university records such as financial reports, human resources information, some research data, unofficial student records (including grade books without SSNs), and budget information.

**Level III data** — Access to Level III institutional data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job, or to those individuals permitted by law. Access to confidential/restricted data must be individually requested and then authorized by the department or unit who is responsible for the data. Level III data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of Level III “Confidential/Restricted” data include official student grades and financial aid data; social security and credit card numbers; individuals’ health information, and human subjects research data that identifies an individual.

## Confidentiality Statements

### Statement for e-mails:

CONFIDENTIALITY NOTICE: This email and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication may contain confidential work product or other legally privileged, confidential or proprietary information. If you are not the intended recipient, please be advised that you have received this message in error and that any use, dissemination, printing or copying of this message is strictly prohibited. If you have received this message in error, please permanently delete it from your computer system and contact the sender at the above address and/or telephone number. Thank you.

### Statement for faxes:

CONFIDENTIALITY NOTICE: The information in this fax is confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this fax is strictly prohibited. If you have received this fax in error, please immediately notify us by telephone and return the original to us at the above address via the US Postal Service.

### Statement for snail mailing:

The information in this package, and any attachments, may contain confidential information and is intended solely for the attention and use of the named addressee(s). It must not be disclosed to any person(s) without authorization. If you are not the intended recipient or a person responsible for delivering it to the recipient, you must not disclose, copy, distribute, or retain this information or any part of it.