# Clarification: Circulating Tenure Dossiers

The purpose of this is to provide guidance to academic units on appropriate ways to make tenure dossiers available to Tenure Committee members and subsequently submit them to our office.

## Guiding Principles

The preeminent concern is that the *integrity* and *confidentiality* of tenure dossiers be maintained. The tenure dossier is the set of documents that is provided to the Tenure Committee for their consideration and forwarded to the Provost for the President's decision. At the time the materials are made available to the Tenure Committee, the tenure dossier includes the following: External Appraisal Letters; Report of the Internal Reading Committee; Report of the Teaching Committee; Student Letters; Letters from Colleagues; Collaborator Statements; and Summary of Evidence. Following committee deliberation, the Statement of Reasons and other required documents as indicated in the Tenure Dossier Checklist are added to the tenure dossier that is forwarded to the Provost for the President's decision.

The tenure dossier must be provided to the Tenure Committee securely so that it cannot be viewed by anyone outside the Tenure Committee or altered in any way*. Of equal importance, the version of the materials in the tenure dossier that is submitted to the Office of the Vice-Provost Faculty & Academic Life for Provostial review and final decision by the President must be exactly the same as the version of the materials that were made available to the members of the Tenure Committee.*

Note: The candidate's teaching and research dossiers may continue to be shared as they normally are with the candidate's permission.

## Strategies for Maintaining Integrity and Security

### 1  Hard Copy Files

The most common and traditional mechanism, which is consistent with confidentiality and file integrity, is to provide Tenure Committee members with full hard copy files of the tenure dossier. More details about hard copy files.

Academic Units should always keep one complete copy of each tenure dossier. Once the tenure process is complete, Chairs should collect and securely dispose of all *extra* hard copy files of each tenure dossier.

### 2  Alternative Mechanisms

The appropriateness of any other mechanism should be measured against the core goal of ensuring the integrity and confidentiality of the tenure dossier. This year there are *two specific approaches (a & b)* identified below that, if used appropriately, can offer comparable security. Pending full rollout of other Microsoft Office 365 features, we may have more options next year.

Blackboard (The Portal) is no longer available. The new content management system Quercus does not allow the creation of non-course-based entities.

## Note:

1.  There must only ever be one version of the tenure dossier materials, whether they are shared in hard copy or electronically.
2.  ***It is important for each Tenure Committee Chair to keep a clear and accurate record of the final contents of the tenure dossier as it was provided to all Tenure Committee members.***
3.  Each Tenure Committee Chair must **keep a master copy of the tenure dossier**, which is a complete copy of the materials shared with the Tenure Committee and forwarded to the Provost's Office. (Again, note that the final version will include additional materials such as correspondence, Statement of Reasons, etc.)
4.  Individual Tenure Committee members may request printed copies of specific materials from the Tenure Committee Chair.

## a.  Hardware Encrypted USB Key (Ironkey)

The ***Ironkey encrypted storage drive*** is the only USB key that IT Services recommends as providing the necessary security for the circulation of the tenure dossier to Committee members. Please do not use other USB keys. More details about Ironkey.

Please note:

1.  It is important that materials be copied to the key as PDFs only**.** Please ask that Committee members not download materials but rather leave them on the key.
2.  When the work of the Tenure Committee is complete, please be sure to delete the materials on each key being careful to retain a full copy of the dossier for your records.

## b.  A Secure OneDrive Folder Within Microsoft 365

Microsoft 365 (M365) was rolled out across the University. This includes the OneDrive platform that will allow for easy, quick, and secure online sharing of confidential tenure materials. Units that can be certain that all members of the Tenure Committee have already been transitioned to Microsoft 365 may wish to use this option. More details about OneDrive.

Once again, please note:

1.  It is important that materials be posted to the site as PDFs.
2.  Please ask that Committee members not download materials but rather leave them within the secure environment.
3.  When the work of the Tenure Committee is complete, please be sure to delete the posted materials from each tenure folder within OneDrive for which you are the administrator, being careful to retain a full copy of the dossier for your records.

# Strategies that are Inappropriate

Other solutions such as Google Drive or Dropbox are not appropriate and should not be used.

# Submission to the Provost's Office of the Tenure Dossier

It is important that Dean's Offices **continue to submit final tenure dossiers in hard copy** to the Office of the Vice-Provost, Faculty & Academic Life for Provostial review and final decision by the President. It is critical that the tenure dossier submitted to our office comprise the same materials and same versions, unchanged, that were provided to and considered by the Tenure Committee.

In addition to the hard copy, it would be helpful if units would also submit an electronic version of each tenure dossier to the Office of the VPFAL using one of the approved mechanisms. When doing so, please ensure the PDFs are optimized for text recognition, without reducing the legibility.

# What to do Following the End of the Review

It is critical once the work of the Tenure Committee is over and a decision on tenure has been reached for the Tenure Chair to:

1. Retain a full copy of the tenure dossier as it was made available to the Tenure Committee members.
2. Collect and confidentially dispose of other hard copies and delete electronic files from all keys or secure sites.