

Date: November 8, 2013

From: Dennis K. Miller

Subj: Intercampus Faculty Council Report – November 5, 2013

To: Faculty Council

The following summarizes important issues for our campus from the November 5 Intercampus Faculty Council (IFC) meeting.

1. IFC continued an ongoing discussion on faculty workload. If our goal is to be an “efficient” university, are we making the best use of our key resource—faculty time? Do we have policies in the collected rules (CRRs) and campus and division bylaws that allow us to or preclude us from establishing workloads for individual faculty members based on their talents and interests and the needs of their division? As resources tighten, is everyone doing their “fair share” or are we asking too much from some faculty members and too little from others?

President Timothy Wolfe mentioned that junior and senior faculty members have consistently complained to him about workload and compensation inequities. He encouraged faculty members to review our post-tenure review policies. This review should not necessarily be focused on punishing or removing faculty, but on reinforcing high-achieving faculty. Can we develop a set of policies at the system, campus and/or division levels that reward faculty at all career stages and provides constructive feedback to those that are struggling?

As part of this effort, Hank Foley (Executive Vice President for Academic Affairs) noted that we may need a cultural change that re-establishes the prestige of teaching. He mentioned that working with students should be valued.

IFC voted to form a task force that will discuss faculty workload and summarize their discussions in February. Dr. Tony Lupo will represent our campus.

2. Deborah Noble-Triplett (Assistant Vice President for Academic Affairs) and Dr. Foley presented background on a challenge UM and MU are facing regarding academic appointments and titles. There have been long-term inconsistencies across the system in how employees are assigned to titles and the responsibilities associated with each title. As a result, the number of UM academic titles has multiplied and we have further complicated the definition of “faculty member”. Are people being recognized for their professional contributions? Are there people whose work does not reflect that of an academic? Who is/should be a UM/MU faculty member?

This has been a long-term confound and Dr. Noble-Triplett and Dr. Foley have proposed a set of goals to begin to resolve it. 1) We need to maintain the integrity of MU/UM faculty titles. 2) We need to provide a clear definition of academic appointments. 3) We need to be sure human resource policies (e.g., vacation and leave) are appropriately applied. 4) We need to ensure that there is alignment with university regulations, policies and practices (including any necessary revisions). 5) We need to have consistency for accurate statistics and reporting (e.g., our AAU concern, budget allocations and strategic planning).

Dr. Foley and Dr. Noble-Triplett have been invited to speak to Council, at length, on this issue after the new calendar year. There is a system-wide task force that will work on this issue with input and leadership from campus constituents.

3. IFC voted to approve changes to the CRRs (2220.020) to allow UM diplomas to have the name of a partnering institution (e.g., UM-S&T offers a degree in collaboration with King Saud University). Initial diploma review will be performed at the respective campus via committees that are comprised (~50%) of faculty members.
4. Beth Chancellor (Associate MU Chief Information Officer and Chief Information Security Officer) reviewed the UM System's data classification policy (a draft version is attached). Briefly, faculty and staff need to consider security across the type of devices (e.g., office desktop through personal smartphone) used to access data. Importantly, personal devices used for work purpose must have the same level of security as campus devices. (Ms. Chancellor is scheduled to discuss this policy with us at the January 23 Council meeting.)
5. Steve Graham (Senior Associate Vice President for Academic Affairs) led the discussion of a proposal for student grade information (e.g., the faculty member's grade book for the semester) is retained for five years (one year is currently required). This change is in response to lawsuits from students and for audits of student financial aid from the federal government. Dr. Graham mentioned that MU already has a policy of retaining data via Blackboard's grade book for five years.
6. Dr. Noble-Triplett demonstrated a new webpage ( [www.umsystem.edu/searches](http://www.umsystem.edu/searches) ) that has suggestions and best practices for successful faculty and administrator searches.

# Desktop, Laptop, and Portable Device Data Classification System Requirements

September 12, 2013

## Purpose of this document

This document outlines and provides an explanation for some of the most important and possibly contentious elements of the proposed data classification system (DCS) for computers, tablets, smartphones, and other portable storage devices such as flash drives and portable hard drives. For the purpose of this document, the term “device” is used generically to describe all types of end-user computers and devices.

This document is intended to provide information about device security and use requirements when such devices are used for work purposes, whether owned by the University or by an individual. It should be noted that it is critical to manage personally-owned devices when used for work purposes in close accordance with the DCS. Improper management of personally-owned devices pose similar risks to University information and data.

### Level 1 and Level 2 information & data

**Devices that only store or access information intended for public consumption or that store or access information/data that is not restricted or confidential in nature, such as budgets, memos, etc.**

**These requirements establish a security baseline for management of all devices.**

**1. A qualified IT professional must setup/provision devices. Users must not change or work around established security settings and security software.**

Some may argue that if the data/information on a device is intended for public consumption, there is no need to professionally manage the device because information is not at risk. However, compromised devices can have a negative impact on other devices, systems and networks so they must be managed and maintained in accordance with basic security standards at all times. IT support staff will be responsible for adherence to established standards.

**2. Ensure device access is handled securely:**

- a. Access devices with full operating systems (i.e., laptops and desktops) via a user’s login ID and strong password.
- b. Access devices with limited operating systems (i.e., certain tablets and smart phones) with a PIN or password. Very simple PINs (i.e., 1111, 1234, etc.) should be avoided.

**3. Devices must not be used as servers.**

The University already has a [DCS for servers](#) that includes more stringent security settings and risk mitigation tools. End-user devices must not be used as servers.

**4. Devices used for work purposes must use Virtual Private Networking (VPN) or other secure connection/transmission technologies when connecting via a public or unsecured wireless network.**

Devices, information and data can be compromised when attached to unsecure or untrusted wireless networks. VPN and other secure technologies can mitigate this risk.

**5. Devices should not be used as a hotspot for other devices to connect to the Internet.**

As with the use of unsecured wireless networks, opening up a device for other users to “join” in order to connect to the Internet subjects both devices to unnecessary security risks.

**6. Lock all devices (i.e., make inaccessible by unauthorized users) and physically secure portable devices when unattended.**

Unlocked devices provide access to systems and applications by unauthorized users and are more likely to be stolen as they are more valuable in an unlocked state.

Laptop and computer peripheral theft is a worldwide problem. The University receives numerous reports of stolen laptops and computer cases. In turn, computer cases often contain flash drives containing University and sometimes personal information and data.

**7. Store all original and/or current versions of data, information, documents, etc. on a University-owned, provided or endorsed system (server) rather than stored on the device.**

This requirement is intended to ensure that original and current copies of work-related information and data are always available to both individual employees and to the University in general. Device failures are common and experience has shown that information/data on a failed device is often unrecoverable. University or departmental application, file and storage servers provide a higher level of assurance for information/data availability and recovery.

**8. Device encryption and/or password protection of sensitive files stored on the device is recommended.**

The central IT department at each campus has encryption tools and services available to encrypt devices. If your device is encrypted and subsequently lost or stolen, at least the information and data on the device will not be accessible. Consult with IT support staff before encrypting a device.

**9. Report lost or stolen devices to the Information Security Office and to Law Enforcement if appropriate. This is a restatement of an existing policy.**

The University is often required to report the loss of certain types of information/data to state and federal authorities. Furthermore, the information security offices at each campus work in conjunction with law enforcement to try to recover devices.

**Level 3 - Restricted information & data**

**Devices that store or access restricted information/data. Examples include but are not limited to student data protected by FERPA, other forms of personally identifiable information (PII) and personnel/HR information and records.**

All requirements detailed previously in this document apply to level 3 devices as well as the following additional requirements:

**1. Special care must be taken when transferring, selling or otherwise disposing of systems that contain level 3 data to ensure compliance with University policies and procedures for surplus/disposal.**

All disposal or transfer activities should be routed through IT support staff who understand how to best dispose of devices and have the tools to ensure they are wiped before transfer. It is important that personally-owned devices be completely wiped when they are no longer needed.

**2. Device encryption is strongly recommended, especially for portable devices.**

The central IT department at each campus has encryption tools and services available to encrypt devices. If your device is encrypted and subsequently lost or stolen, at least the information and data on the device will not be accessible. Consult with IT support staff before encrypting a device.

**3. International Travel**

It is highly recommend that employees not travel internationally with sensitive or restricted data on their device(s). Consult the [information security travel standards](#) as well as your IT professional for additional assistance.

**Level 4 – Highly Restricted information & data**

**Examples of highly restricted data include patient information (HIPAA), social security numbers, credit card numbers, and biometric data.**

All requirements documented previously in this document apply to level 4 devices as well as the following additional requirements:

**1. Must be managed by a qualified IT professional**

**2. Device encryption is required.**

All devices storing or accessing level 4 information and data must be encrypted. Devices that do not support encryption are not authorized to access level 4 information and data. Typically, devices that can't be encrypted are obsolete and should be replaced with more current technology.

The central IT departments at each campus have encryption tools available for use on University-issued devices. Consult with IT support staff before encrypting a device.

**3. Devices, if capable, must deploy an automatic wipe after a certain number of bad login attempts. Recommended wipe at 10 attempts.**

Supporting Information:

Information Security Policy: [http://www.umsystem.edu/ums/rules/bpm/bpm1200/manual\\_1203](http://www.umsystem.edu/ums/rules/bpm/bpm1200/manual_1203)

UM Information Security Program: <http://infosec.missouri.edu/>

Information Security Officers: <http://infosec.missouri.edu/admin/iso.html>

Data Classification System (DCS): <http://infosec.missouri.edu/classification/>