**DRAFT Review of PG-55 Update -- April 16th, 2024**

**Faculty Welfare & Concerns Committee**

This is a compilation of questions and concerns from individual faculty, the Faculty Senate Executive Council, and the membership of the Faculty Welfare & Concerns standing committee.

**General Issues**:

Has this draft been reviewed yet by University Counsel? Some things seem to be dubious in a legal sense and problematical from an enforcement perspective.

Many references are made to "sensitive data" or "sensitive information" throughout all ~~of~~ the documents. The following additional elements are necessary.

- definitions for "sensitive data" and "sensitive information"
- a set of criteria for identifying something as "sensitive"
- who gets to designate something as sensitive
- when public documents are treated as "sensitive" a written explanation of how they could be misused is required to be made public in place of having them available to the public.
- a procedure for periodic review of the categories of information/data designated sensitive so public debate can influence whether a type of information remains "sensitive"

**IT Response:** Sensitive data can be many things but generally this involves some sort of Personal Identifiable Information (PII). There are cases where a combination of non PII can be assembled to form enough detail to become PII. The intent of these policy statements are to ensure that all parties attempt to understand the data being consumed and act appropriately.

**Specific Issues**:

*Line 66* --"obtain additional resources beyond those allocated."

**What does this mean?**

**IT Response:** This policy statement is designed to prevent a user from purposely accessing resources that they know they are not supposed to have access to or were not officially granted access to by the system owner/administrator with proper approvals.

*Line 81* -- "Personnel should not intentionally access, create, store, or transmit material which Morehead State University may deem to be offensive, indecent, or obscene."

**Who will be the arbiter for this?**

**IT Response**: Local, State or Federal law enforcement.

*Line 89* -- "All remote access connections made to internal Morehead State University networks and/or environments must be made through approved, and Morehead State University-provided, virtual private networks (VPNs)."

**Does this mean that we cannot access MSU things from our homes?**

**IT Response**: The intent is to provide all users with basic secure VPN access to the internet at some point in the future. Specific access to enterprise systems such as Ellucian Colleague and other on-prem resources will be accessible through the VPN but will require an approval process for that additional access.

*Line 96* – "Personnel must not share their Morehead State University authentication information, including:

- Account passwords,
- Personal Identification Numbers"

Some university business (filling out travel requests, contacting payroll, getting help with IT issues) require personnel to share their MSU ID #. This IT policy, though, says we are *never* to share that ID #.

**IT Response**: Sharing individual technology account passwords (aka your m+7 account) is forbidden. If there is a shared resource, then additional access credentials should be approved and obtained for that sharing process from OIT. With some systems such as Microsoft Office 365 it is understood that the design of the system allows for m+7 account numbers to be exposed or shared with other users. In these cases, it is acceptable to share your MSU ID.

*Line 162* -- "Any personal use of Morehead State University provided email should not: Be associated with any political entity, excluding the Morehead State University sponsored PAC."

Enforcement seems problematical. Who will be the arbiter?
Hypotheticals that are all apparently violations of this regulation:

- A staff sponsor of the College Republicans student group sends out an email announcing an ice-cream social.

- A faculty member monitors the KY General Assembly during one of its sessions and reports what they learn from this in an e-mail to colleagues.

- A union organizer on staff sends announcements to campus e-mail addresses.

- The College Democrats want to get the vote out and use campus e-mail to known supporters.

**IT Response**: The intent is to stop employees from misrepresenting Morehead State University as having a political bias or aligning its values with a political agenda. It has nothing to do with employees' communications with their preferred political groups.

*Line 173* -- "Personnel should use discretion in disclosing confidential or internal information in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data."

**When the policies talk about not disclosing "internal telephone numbers" does this mean we aren't supposed to give people our office phone numbers?**

**IT Response**: The statement specifically spells out that some "**discretion"** needs to take place in our daily work environments. Some individuals at MSU have multiple phone numbers. Some are for public consumption and the others intended to be private (aka not typically put in a public directory). In this case the policy is asking for discretion when handing out those type of numbers that are designed not to be in a public directory. Also, when consulting with COMA on the public website, it is critical to only publish user specific data that cannot be used for malicious use. If you post your name, address, phone number and email, there are systems that "scrape" the web pages and then add you to telemarketers that are both annoying and, in some cases, bad actors trying to lure you into losing money or resources. Data that is publicly exposed should be kept to the minimum amount of data to get the job done. University Directories with individual numbers will not be exposed and will aways require a login to access.

*Line 186* -- "The Internet must not be used to communicate Morehead State University confidential or internal information, unless the confidentiality and integrity of the information is ensured, and the identity of the recipient(s) is established."

**A definition for "confidential information" and "internal information" and a set of criteria for identifying it and who gets to designate something as such are needed.** [SEE General Issues]

**IT Response**: These are defined under the state and federal law related to the following:

**FERPA**: Family Education Rights and Privacy Act
**HIPPA**: Health Insurance Portability and Accountability Act
**GLBA**: General Data Protection Regulation (EU Citizens)
**CCPA**: California Consumers Protection Act (California Residents)
**PCI/DSS**: Payment Card Industry/Data Security Standard
**PIPEDA**: Personal Information Protection and Electronic Documents Act (Canadian Citizens)

These are not 100% inclusive but are representative of the rules that MSU is governed by in various departments and roles.

*Line 190* – “Use of the Internet with Morehead State University networking or computing resources must only be used for business-related activities.”

**“Business-related activities” does not automatically allow for academic freedom in teaching and research. If I connect to the Internet using MSU resources looking for adaptations of Jane Austen novels, that’s not a “business-related activity.” It is through ~~though~~ a teaching related activity ~~as~~ that I prepare for my fall classes.”**

**IT Response**: Academics is the business of MSU and thus any use of the internet in the pursuit of academic work is acceptable. This statement should have no bearing on academic freedom in teaching and/or research.

*Line 213 - 225*

- “Morehead State University OIT Leadership may choose to execute “remote wipe” capabilities for mobile devices without warning. **IT Response**: Revised statement: In consultation with the device owner, Morehead State University OIT Leadership may choose to execute “remote wipe” capabilities for mobile devices.
- If there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the personnel’s possession as part of a formal investigation. **IT Response**: Revised statement: If there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the personnel’s possession as part of a formal investigation by local, state or federal authorities.
- All mobile device usage in relation to Morehead State University Information Resources may be monitored, at the discretion of Morehead State University OIT Leadership. **IT Response**: We log all connections and all data traffic to and from MSU Information Resources. OIT does not have visibility into the payloads of the connections.
- Morehead State University OIT Support for personally owned mobile devices is limited to assistance in complying with this policy. Morehead State University OIT Support may not assist in troubleshooting device usability issues. **IT Response**: We will assist with configuration and troubleshooting of problems related to the authorized access of MSU information resources.

- Use of personally owned devices must follow all other Morehead State University policies. **IT Response**: Should we encounter an ongoing problem with the use of personally owned devices and a **future policy** to mitigate the problem is proposed and approved, then all personally owned devices used for MSU business-related activities will be subject to that policy.

- Morehead State University reserves the right to revoke personally owned mobile device use privileges if personnel do not abide by the requirements set forth in this policy." **IT Response**: If you are storing MSU business-related data on your personal device, the protection of that data is still under the purview of MSU.

Will we need to install special software onto our devices simply to access the network?

**IT Response**: No. VPN access from off campus will only be permitted via the use of an MSU issued device. Access may be prevented if the device has a critical vulnerability and cannot be patched remotely.

**Is there going to be a guest network for our personal devices?**

**IT Response**: There is already a guest network, however that network (by design) has zero access to Ellucian Colleague and other on-prem MSU resources.

**If we cannot use our cell phones to monitor emails it will become difficult for those of us teaching online classes. Will the university provide us with a cell phone in addition to our computers for university use?**

**IT Response**: Use of MSU issued devices to check email is permitted on or off campus using any available connection to the internet. Check with Dean or Dept. Chair about a university issued phone.

**How will the administration respond when students complain about their professors being inaccessible, as a result of us not being permitted to use personal devices to access the internet or even our MSU devices off campus?**

**IT Response**: Use of MSU issued devices to check email is permitted on or off campus using any available connection to the internet.

**What are departmental social media managers supposed to do when our devices are no longer permitted to be used for MSU purposes (most social accounts are only fully accessible from mobile devices)?**

**IT Response**: Per request from Deans/Dept. chairs, MSU issued mobile devices can be provisioned.

**Does this mean that if we use our personal cell phone to access MSU systems (such as e-mail**

**or Blackboard or the LiveSafe App), then MSU could choose to delete everything on our personal cell phone (including all photos and videos, and all names and phone numbers in the Contacts list) at any time, without any advance notice to us?**
**IT Response**: We revised the statement related to this question. The new language adds "in consultation with the device owner."
**Is this only if the mobile device is suspected of being used to cause the incident or breach, or does it include situations where the mobile device was simply affected by an incident or breach that was caused by someone else?**

**IT Response**: We revised the statement related to this question. The new language adds "in consultation with the device owner". If there is a need to protect MSU data then a wipe can be issued. That may be due to an incident or possibly the root cause of an incident. Either way, the device owner would be consulted.

**If IT can access information on any device connected to its network, what privacy do students have? They can't do their work without a personal device, and their tuition helps pay for the network. Now, after we require them to use personal devices to access a network even when we're in something like a computer lab, we're leaving them open to Big Brother surveillance.**

- **Scenario:** a young female student is in Starbucks, completing homework for her class on her laptop. She's connected to MSU secure and working in the **BlackBoard system. While she is working, she gets a text from her friend which pops up on her laptop. This personal text involves an aspect of her reproductive health. She responds to this text using the MSU secure system. What's to stop MSU from getting or handing over that personal text to a zealous Attorney General who is seeking records related to all miscarriages or anything that could be construed as "gender affirming care"?**

  **IT Response**: MSU has no means, desire, or legal permission to intercept network traffic on a Starbuck's network. MSU OIT monitors network traffic but not contents of the payload of the traffic. The text message data referred to here is encrypted between the student's machine and SMS/Text messaging provider and is not capable of being decrypted by MSU OIT Network or Security staff.

**Remote wiping.** The policy doesn't differentiate between mobile devices owned by MSU and those that people bring in. So, we're seriously saying that IT is prepared to (and capable of) remotely wiping person devices if people violate IT polices?

**IT Response**: Revised statement: It is recommended that all personally owned laptops and/or workstations be onboarded to Morehead State University's mobile device management, anti-virus, and anti-malware solutions if they are to be utilized with Morehead State University information systems.

BYOD devices are not mandated to be managed by MSU. Any device owned by MSU is managed by the mobile device management platform utilized by OIT.

- **How does IT have control of the operating systems of personal devices?**
- **Why does IT have control of the operating system of personal devices?**
- **What gives IT the right to destroy personal property?**
- **How is this not a violation of rights, especially the rights of students?**

**Civil asset forfeiture:** "If there is a suspected incident or breach associated with an mobile device, it may be necessary to remove the device from the personnel's possession as part of a formal investigation." **So, IT is now the police? On what authority? And what's will the passive voice here?**

**IT Response**: MSU issued devices are the property of MSU. BYOD devices are not mandated to be managed by MSU but are subject to the best practices spelled out in this document and if the device has MSU data on it, it could be included in any formal investigation handled by law enforcement agencies.

*Line 227* – "Photographic, video, audio, or other recording equipment, such as cameras in mobile devices, is not allowed in secure areas."

**IT Response**: Pictures in/of our data center, data equipment closets, and/or other areas are not permitted. There may be other areas on campus when photos are not permitted but within OIT those areas are limited to our datacenters.

How are "secure areas" defined?

**IT Response**: Revised Definition added to PG-55: **Secure Area -** A secure area is a designated physical space or location that is protected and controlled to prevent unauthorized access. The primary purpose of a secure area is to safeguard sensitive information, valuable assets, or critical infrastructure from theft, sabotage, espionage, or other security threats. Secure areas can vary widely in size and complexity, ranging from small rooms or compartments within a building to entire facilities or compounds. Access to these areas is typically restricted to authorized personnel only, who may be required to undergo identity verification, authentication, or other security measures before entering.

***Line 276 --***

> "As a convenience to Morehead State University personnel, incidental use of Information Resources is permitted. The following restrictions apply:
>
> - No files or documents may be sent or received that may cause legal action against, or embarrassment to, Morehead State University or its customers."

**Who are Morehead State University's "customers"? This is an odd word to use at a not-for-profit educational institution.**

**IT Response**:  Please see the "Scope" portion of the policy:

BEGIN POLICY STATEMENT
SCOPE:
This policy applies to the use of information, devices, services, and technology accounts to conduct Morehead State University (MSU) business or interact with associated networks and business systems, whether owned or leased by MSU, the employee, or a third party. All faculty, staff, students, contractors, consultants, temporary, and other workers at MSU and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, devices, services, and technology accounts in accordance with MSU policies and standards, and local laws and regulations.

This policy applies to faculty, staff, students, contractors, consultants, temporary, and other workers at MSU, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by MSU.
END POLICY STATEMENT

Customers is a broad term used to capture everybody in the scope statement.

**How can anybody accurately predict litigation or "embarrassment"?**

**IT Response**:  This policy was revised to support a **proactive**, rather than a **reactive** model of information security posturing. Avoiding unnecessary bad publicity or embarrassment is key to protecting the enrollment, retention, and subsequent cash flow goals of Morehead State University.

**Is reporting a crime a violation of university policy?**

**IT Response**:  No.

**References to institutional "reputation" and "embarrassment" are overly broad and tend toward censorship. Who or what determines a "potential" toward the harm of a reputation?**

**IT Response**:  The policy uses words like "discretion" whenever possible. The intent is to engage users critical thinking skills when they are dealing with communications, data, devices and MSU resources to help protect MSU and its reputation as an outstanding teaching university.