The University of Southern Mississippi
Faculty Senate Meeting Agenda
Friday, May 3, 2019, 2:30 p.m.
Trent Lott National Center 101/102 (Hattiesburg)
IVN to North Academic Building 125 (Gulf Park) and
Stennis Building 1103 Center for Higher Learning Conference Room
Friday, December 14, 2018, 2:00 p.m.
Union Hall of Honors (Hattiesburg), IVN to North Academic Building 125 (Gulf Park)


Absent: Miles Doleac, Tim Rehner, Mike Morgan, Ashley Krebs

1.0 Organizational Items
   1.1 Call to Order: The meeting was called to order by Mac Alford
   1.2 Roll Call
   1.3 Recognition of Quorum (20)
   1.4 Recognition of ⅔ membership for voting on Bylaws and Resolutions (26)

2.0 Adoption of Agenda: Approved unanimously by voice vote

3.0 Program
   3.1 Rodney Bennett, President (not available)
   3.2 David Sliman, Chief Information Officer (updated iTech policies)
      - Mr. Sliman addressed senator questions about the iTech policy proposals included in Appendix A and B.
      - Specifically, 4.3 and 4.4 were addressed and people should be aware that they should copy important emails.
      - 3.4: Purpose of 3.4 is to eliminate the thread of someone taking over the account that is no longer being used.

   3.3 Aaliyah Elbert, SGA initiatives
      - Ms. Elbert addressed the senate and read a letter from the SGA president about the class schedules.
      - Ms. Elbert addressed the proposed resolution about the mandatory reporting statement to be part of the syllabi and the resolution to have a title IX requirement statement.
4.0 Approval of Minutes: **Approved** unanimously by voice vote

4.1 April 2019

5.0 Officer Reports

5.1 President (Mac Alford):
- President Bennett wants to hold a summit on the schedule.

5.2 President-Elect (Susan Hrostowski): No report

5.3 Secretary (Melinda McLelland): No report

5.4 Secretary-Elect (Amber Cole): No report

6.0 Decision / Action Items

6.1 June 7, 2019 meeting: The Senate will hold a meeting on June 7, 2019 due to the need to finalize elections and seat new senators.

7.0 Standing Committee Reports

7.1 Bylaws (Kim Ward)
- Discussion of edits to by-laws proposed by the committee.
- There was a motion and a second to remove “vacancy” from 2.9.2. All were in favor.
- There was a motion and a second to change 2.3.4 to “for three years”. All were in favor.
- There was a motion and a second to change 2.9.3 to “university approved absence”. All were in favor. The discussion included absence reasons for medical, military, maternity/paternity, parental, FMLA, etc.
- All were in favor of adopting new by-laws of faculty senate.

7.2 Elections

7.2.1 General Report / Update (Tom Rishel)
- The Elections Committee coordinated with Mike Barry, Megan McCay, and the chairs of the other advisory bodies to produce both the opt-in ballot as well as the final ballot. This is the expected timeline for the elections process.
- 5/3 (Friday): Launch opt-in ballot
- 5/10 (Friday): Close opt-in ballot
- 5/13 (Monday): Mike Barry will send out results from opt-in ballot to election committee members
- 5/16 (Thursday): Each council tells Mike who will be on the ballot and election committee provides aggregated candidate bio info statement document for those bodies who require candidate bios
- 5/17 (Friday): Launch round 1 ballot
- 5/24 (Friday): Close round 1 ballot
7.2.2 Officer Elections
   7.2.2.1 President-Elect: Lilian Hill was nominated, nominations were closed, and Lilian Hill was voted by acclimation
   7.2.2.2 Secretary-Elect: Kim Ward was nominated, nominations were closed, and voted by acclimation

7.3 Handbook (David Holt): David Holt reported as outside committee member. He asked the senators look through document, share with colleagues, and provide feedback to him.
   7.3.1 Reorganization Initiative #3:
   7.3.2 Faculty Handbook
   7.3.3 Faculty Handbook Committee Bylaws

7.4 Academics (Catherine Bomhold):
   • Catherine shared feedback from the online education committee’s first meeting

7.5 Administrative Evaluations (Melinda McLelland):
   • Evaluations will be emailed/delivered by next week

7.6 Awards (Bradley Green):
   • Award are all done for the year

7.7 Finance (Amber Cole):
   We had a meeting with the VPFA, Allyson Easterwood, on Friday, April 26\textsuperscript{th} and we discussed the upcoming employee pay raises.
   The following groups are \textbf{not} eligible for the pay adjustment:
   1) Any employee who received a pay increase, for any reason, between 12/31/2015 and 12/31/2018 - An employee who received a pay increase before or after this time period is still eligible (assuming he/she meets the other criteria).
   2) Athletic department employees.
   3) Adjunct, part-time, and student employees.
   4) Any employee hired after 12/31/2015.
   After eliminating these groups, approximately one-third of all full-time employees will be eligible to receive the pay increase.
   If eligible, the increase will be 2\% of the employee’s salary as of 1/31/2019.

A more descriptive summary from Krystyna Varnado was sent to department heads and was as follows:
   ☐ The state set the eligibility requirements and there can be no exceptions- only the people on the list are eligible (money cannot be transferred to someone else) and each person on the list will receive 2\% (no adjustments or take-aways).
   ☐ Only employees hired full time by December 31, 2015 (and have stayed FT with no break in service) were considered eligible.
Employees who received a raise between December 31, 2015 and December 31, 2018 were not eligible. Any raise for any reason took the person off the list, per the state rules. The state made no exceptions for “unfair” situations.

Anyone who met the above criteria who has received a raise since December 31, 2018, is considered eligible (the parameters were between specific dates). However, the raise is based on their salary as of January 31 and then will be added to whatever their current rate is (so not 2% of their current rate if the raise happened after January 31).

The effective dates will be:
- Exempt: July 1 (the first day of the first full pay period in the fiscal year)
- Non-Exempt: July 13 (first day of the first full pay period in the fiscal year)
- Faculty: September 1 (this raise only impacts the primary job so summer pay is not impacted)

7.8 Governance (Don Redalje): No Report

7.9 Gulf Coast (Lee Follett): No Report

7.10 University Relations and Communication (Nicolle Jordan): No Report

7.11 Welfare and Environment (Bryan Lapierre):

7.11.1 Schedule Summit, this summer

- Bryan shared the sense of the senate letter. There was no further discussion. All voted to send the letter forward with none opposed.

President Rodney Bennett
Cc Provost Steve Moser

Subject: assessing the new schedules

Dear Mr. President,

The good news that retention rates are up comes at the same time that both students and faculty have serious concerns about the effectiveness of the new class scheduling. In order to help assess the pluses and minuses of the scheduling, the Faculty Senate recommends a four-part action plan:

1. Provost’s “Summit” this summer on scheduling. The Senate endorses this as a good first step. Student and faculty representatives should be part of the Summit.

2. Survey analysis. The Faculty Senate will have results of a survey on scheduling soon. The SGA is planning to query students next fall. Results from both surveys are critical to gathering data from the principle parties affected by the revised
academic calendar and can be used to identify strengths, weaknesses, and possible areas for change.

3. Open meetings. The Faculty Senate endorses the idea of you and the Provost being present at open meetings on campus for (a) students and (b) faculty on scheduling.

4. Data. The rise in retention rates is certainly good news. Data on the trend in student visits to campus mental health services and the enrollment in Study Abroad would also be useful to know as well as other data that might be collected on scheduling. Data also needs to be evaluated on the intersession periods created by the reform of the academic calendar. For example, is there an increase in intersession enrollment? What are the failure, withdrawal, and drop rate in those sections?

Sincerely,

Mac Alford, Faculty Senate President

- Cindy Handley asked for comments about the faculty survey she shared with the Senate earlier. No further discussion. The senate voted to send out the survey with none opposed.

8.0 Outside Committee Reports: None (Handbook Committee reported earlier)

9.0 Reports from Other University Advisory Bodies: None

10.0 Consent Items
   10.1 Kate Greene (Social Science & Global Studies) to stand in for Bob Press
   - All voted in favor of accepting Kate as a one year replacement for Bob.

11.0 Unfinished Business
   11.1 None

12.0 New Business
   12.1 None

13.0 Good of the Order

14.0 Announcements
   14.1 Next Senate Meeting, if confirmed: June 7, 2:00 p.m., Cook Library 123 with IVN to North Academic Building 125 (Gulf Park)
   14.2 Senate Executive Committee, TBD
   14.3 Next Staff Council meeting: June 6, 9:30–11:00 a.m., Trent Lott 207
   14.4 Commencements, May 9 (graduate), 10 (Hattiesburg), 11 (Gulf Coast)
Appendix A:

Email Use Policy

Policy Statement

The University email service supplies email, calendaring, contacts, and email list services in support of the University's mission of education, research, and public service and it is used to conduct University business. Access to and use of university systems is a privilege accorded at the discretion of the University. Use of university email service is subject to legal and policy restrictions that apply to all University email address holders.

Reason for Policy/Purpose

The reason for this policy is to effectively communicate the University policy regarding the use of the University email service for academic, research, and official administrative activities.

Who Needs to Know This Policy

All students, faculty, staff, and any other University of Southern Mississippi email address holder.

Website Address for this Policy

https://www.usm.edu/institutional-policies/policy-adma-it-001

Definitions
**Data Owner:** Entity or individual with authority and accountability of data collection, generation, access, and use.

**Email:** Refers to “electronic mail,” which is correspondence between individuals through electronic means. Email created or received as part of University business are University records and the property of the University.

**Information:** Local and cloud-based documents and communications, including emails, calendars, contacts, voice mails, and their associated metadata, which are in files and accounts associated with a user. This would include all emails and their attachments in a user’s inbox, sent items folder, or other email folders that are recognized as part of the account associated with a user, and all documents in that user account’s electronic folders.

**Spam:** unsolicited bulk electronic messages.

**University Business:** USM-Mailouts, emergency alerts, class information, communication to and from students, faculty, and staff, and other business directly tied to The University of Southern Mississippi.

**University Systems:** All electronic services, networks, and devices owned, provided, or administered by the university, such as email services, Internet access, file servers, voice message services, storage devices, laptop and desktop computers, phones and other mobile devices, including usage and access logs.

### Policy/Procedures

1. **Usage and Requirements**
   1.1. At the directive of the University Executive Cabinet, all University employees must use their “@usm.edu” email account for all correspondence regarding, or relating to, University business or academics.
   1.2. University employees must not redirect (forward) their USM email to another USM email account or non-USM email service (e.g. Hotmail, Gmail, Yahoo, AOL, etc.).
   1.3. Email is provided as a professional resource to assist students, faculty, and staff in fulfilling the educational, research, and service goals of The University of Southern Mississippi. Each user is responsible for using the email service in a professional, ethical, and lawful manner.
   1.4. Students may use the University email services for personal use, so long as that use conforms to the University’s Acceptable Use Policy (AUP) (Policy: ACAF-IT-010).
   1.5. Personal use of University email services by USM employees is strongly discouraged. Any personal use should be incidental, must not interfere with assigned duties, and must comply with the AUP.

2. **Email Communications and Students**
   2.1. All students will be assigned an “@usm.edu” email account at the time of enrollment.
2.2. Students must understand that USM will use the student’s “@usm.edu” email address for communication. Students are expected to use their “@usm.edu” email accounts for correspondence with faculty and staff.

2.3. Faculty will determine how email will be used in their classes and should specify their requirements in course syllabi. Faculty can assume that students' official "@usm.edu" accounts are being accessed and faculty can use email for their classes accordingly.

2.4. The dissemination of mass email to students at USM will be restricted to University business. Authority to approve the distribution of email in this manner rests with the Office of University Communications and University administration.

2.5. Students may forward their USM email account to a non-USM email account at their own risk. The University will not be responsible for the handling of email by non-university email services. Email redirection does not change the individual’s responsibility for reading and responding to official communications sent to the student’s “@usm.edu” address.

3. Email Ownership and Access

3.1. Email created, received, or stored in University managed email accounts are the property of USM and the State of Mississippi, and may be subject to public records requests. For this reason, the privacy of personal and non-university information cannot be guaranteed if transmitted through or stored in University systems or services.

3.2. Access to and use of “@usm.edu” email accounts may be suspended or terminated, at the discretion of the University or if requested by the employee’s supervisor, University Police Department, Human Resources, or General Counsel.

3.3. Emeriti may have access to and use of their “@usm.edu” email account indefinitely.

3.3.1. Emeriti will lose access to and use of their “@usm.edu” email account if the account is not accessed for more than one (1) year.

3.4. Faculty, including adjunct faculty, may have access to and use of their “@usm.edu” email account for one (1) year after voluntary termination of their contract or employment.

3.5. Students may have access to and use of their “@usm.edu” email account for one (1) year after the end of the last semester the student completed.

3.6. Affiliates are allowed access to and use of a “@usm.edu” email account. Individuals entered as affiliates must have designated account start and end dates, not to exceed one (1) year. Reaffirmation is required to extend an account beyond one (1) year.

3.7. Staff, retirees, affiliates, and other employees, who are not faculty or students, will lose access to and use of their “@usm.edu” email account upon termination.

3.8. Email data of current or former employees may be provided to the University administration or the employee’s supervisor for business continuity or investigative purposes.

3.8.1. Requests for such data can only be made by the employee’s supervisor, the University Police Department, Human Resources, or General Counsel.

3.8.2. Requests must be submitted in writing to the General Counsel.

3.9. Email data of deceased or incapacitated students may be provided to an authorized individual.

3.9.1. Authorized individuals include an executor or a person who holds power of attorney for the student.
3.9.2. The authorized individual must provide a legal document demonstrating authorization.

3.9.3. The request must be submitted in writing to the Office of the General Counsel.

3.10. The University will not recover or provide access to email for an individual after their access has been removed.

4. **Retention**

   4.1. iTech will archive email sent to or from an “@usm.edu” user address for three (3) years. After three (3) years, the archived email will be expunged.

   4.2. The value of an email message is determined by its informational content.

   4.3. The length of time for which email is retained is based on its value to the University in conducting its business activities, complying with and fulfilling and ensuring its legal rights and obligations, fulfilling fiscal requirements, and in some cases, documenting the history of the University. For guidance, personnel must refer to the General Records Schedule (http://www.lib.usm.edu/spcol/records_retention.html) or any special records schedule issued for their office.

   4.4. It is the responsibility of the Data Owner to ensure emails are archived appropriately, as required by the General Records Schedule.

5. **Abuse**

   5.1. Users may report the receipt of spam by forwarding the offending email, preferably as an attachment, to: spam@usm.edu.

   5.2. Recipients of spam, or other policy violating email originating from an “@usm.edu” email address may forward the offending email, preferably as an attachment, to: abuse@usm.edu.

6. **Violations and Penalties**

   6.1. Any student, faculty, or staff found to have violated this policy may be subject to disciplinary action in accordance with procedures defined by USM administrative policies stated in the handbook governing that individual.

   6.2. Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract.

---

**Appendix B:**
Acceptable Use Policy

Policy Statement

The University of Southern Mississippi (USM) is committed to protecting its information technology (IT) resources and the students, faculty, staff, affiliates, contractors, vendors, and guests from illegal or damaging actions by individuals, either knowingly or unknowingly. Inappropriate information technology use exposes USM to risks including, but not limited to, malware, compromised accounts of networked systems and services, compliance and regulatory issues. Effective information security requires the participation and support of every USM student, employee, or other who handles University data and/or information technology resources.

Reason for Policy/Purpose

This policy is required for the effective communication of the University policy regarding the acceptable use of information technology resources at USM.

Who Needs to Know This Policy

This policy applies to students, faculty, staff, affiliates, contractors, vendors, and guests at USM, including personnel affiliated with third parties or individuals accessing University IT resources.

Website Address for this Policy

usm.edu/institutional-policies/policy-ACAF-IT-010

Definitions
**Antivirus Software:** software specifically designed to detect and remove computer viruses and malware.

**Information Technology Resources:** any computing device, network, or network service used for creating, reading, sharing, modifying, or storing data and information.

**Malware:** malicious software that is intended to damage or disable computer systems.

**Password:** a combination of letters, numbers, and symbols, used to authenticate an individual.

**Spam:** unsolicited bulk electronic messages.

**Users:** students, faculty, staff, affiliates, contractors, vendors, and guests.

---

**Policy/Procedures**

1. **Ownership and General Use**
   1.1 University information technology resources (IT resources) are provided for users to enable, support, or enhance the mission and goals of the University. Use of IT resources by individuals unaffiliated with the University is prohibited, except for IT resources that are explicitly made available for use by unaffiliated individuals.
   1.2 Users of University IT resources must exercise good judgment regarding incidental personal use and activity not related to the mission and goals of the University.
   1.3 USM will ensure individuals have a reasonable degree of privacy while using IT resources, phone services, and internet or network services; however, data, documents, and email created, received, or stored on University IT resources, including services hosted by a third party for use by USM, will be considered the property of USM and the State of Mississippi, and may be subject to public records requests. For this reason, the privacy of personal and non-university information cannot be guaranteed if transmitted through or stored on a University IT resource or service.

2. **Responsibilities**
   2.1 Users of University IT resources are responsible for knowing and understanding any laws, regulations, policies, or contracts that may affect or govern the resources they use or the information they may access, create, or modify.
   2.2 Users are expected to utilize IT resources with integrity and respect for other individuals, institutions, and entities.
   2.3 Users must take necessary steps to prevent unauthorized access to University information and resources.
   2.4 Users are responsible for the security of their account credentials, including passwords and passphrases. Users are expected to keep their credentials private and must never ask another user for their University account credentials.
3. **Acceptable Use**
   3.1 Use of University IT resources that enables, supports, or enhances the mission of the University, fulfills the expected duties of an employee, or aids in the scholarly pursuits of a student, is generally acceptable.
   3.2 Extracurricular activity that does not disrupt or harm University business or expose the University and its resources to unacceptable levels of risk, are generally acceptable.

4. **Unacceptable Use**
   4.1 The following activities including, but not limited to, are strictly prohibited:
      4.1.1 Use of University IT resources to engage in any activity that is illegal under local, state, federal, or international law.
      4.1.2 Collection, storage or distribution of pornography or material considered to be obscene, for purposes not related to University sanctioned academics, research, or legal proceedings.
      4.1.3 Unauthorized copying, sharing, or downloading of any material or intellectual property protected by copyright or trade secret, including, but not limited to, digitization and distribution of photographs or text from magazines, books or other copyrighted sources, copyrighted music, copyrighted movies, and the installation of any copyrighted software for which USM or the end user does not have an active license.
      4.1.4 Intentionally exposing University IT resources to malicious software.
      4.1.5 Sharing access to University accounts, resources, and login information with others or allowing use of accounts or services by others.
      4.1.6 Using University IT resources to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws.
      4.1.7 Effecting security compromise, where compromises include, but not limited to, accessing data for which the user is not authorized, allowing information or resources to be available to unauthorized users, or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties.
      4.1.8 The disruption of network resources including, but not limited to, ping floods, packet spoofing, denial of service attacks, and the forging of routing information.
      4.1.9 Port scanning or vulnerability scanning is expressly prohibited unless prior notification is given to USM Information Technology Services (iTech) or these processes are within the scope of regular duties.
      4.1.10 Executing any form of network monitoring which will intercept data not intended for the individual, unless this activity is within the scope of regular duties.
      4.1.11 Providing information about (or lists of) USM faculty, staff, or student non-directory information to parties outside the University without the express written permission of the University administration.
      4.1.12 Sending email messages, including "spam" or other advertising material, to individuals who did not specifically request such material.
4.1.13 Any form of harassment via email, messaging service, forum, or social media; whether through language, frequency, or size of messages.
4.1.14 The forging of email header information in an attempt by an individual to misrepresent or hide his or her identity.
4.1.15 Creating or forwarding chain letters or other pyramid schemes of any type.
4.1.16 Use of University resources to advertise any service or product not provided by USM, for personal gain.

5. Enforcement
5.1 Students faculty, and staff: Any student, faculty, or staff found to have violated this policy may be subject to disciplinary action, up to and including suspension, expulsion and/or termination of employment in accordance with procedures defined by USM administrative policies stated in the handbook governing that individual.
5.2 External Entities: Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract.