QUORUM = 7

Marshall University Faculty Senate
Executive Committee Agenda
Monday, March 10, 2025, 12:00 Noon
MSC 2W16b/Microsoft Teams

1. Approval of Proposed Agenda
2. Approval of Minutes of February 10, 2025
3. Announcements – Chair
4. Recommendations/Resolutions
    a. **SR 24-25-23 BAPC** Recommends amending **UPAA-2 (Class Attendance).**
    b. **SR 24-25-24 BAPC** Recommends amending **UPGA-2 (Inclement Weather).**
    c. **SR 24-25-25 CC** Recommends approval of the listed **UNDERGRADUATE PROGRAM ADDITION, DELETION, CHANGE** in the following college and/or schools/programs: **BA, Music Industry; Music Management; Athletic Training; Biomechanics; Exercise Science; Strength and Conditioning; Kinesiology; AT, Pre-Physical Therapy; AT, Pre-Med; AT, Pre-Physician Assistant; Biomec Pre-Physical Therapy; Biomec, Pre-Med; Biomec Pre-Physician Assistant; Ex Sci, Pre-Physical Therapy; Ex Sci Pre-Med; Ex Sci Pre-Physician Assistant; SC, Pre-Med; SC, Pre-Physical Therapy; SC, Pre-Physician Assistant; Kin, Pre-Physical Therapy; Kin, Pre-Med; Kin Pre-Physician Assistant; BS, Health and Movement Sci Degree; Pre-Computer IT (Non-Deg); BFA, Music; Perform, BFA Music Emphasis; Jazz Studies, Emphasis; Multidisciplinary Studies; Music Entrepreneurship; Social Work; BS, Professional Pilot.**
    d. **SR 24-25-26 CC** Recommends approval of the listed **UNDERGRADUATE COURSE ADDITION, DELETION, CHANGE** in the following college and/or schools/programs: **MUSP 225; MUSP 475; DTS 315; CHM 425; PS 101L; ART 218; MUS 101; MUS 110; MUS 326; MUS 495; MUS 310; MUS 327; MUS 427; NUR 418; PS 101.**
    e. **SR 24-25-27 APC** Recommends approval of **ITP for BS in Sonography.**
    f. **SR 24-25-28 EC** Recommends amending **UPGA-10 (Information Security).**
5. Set Agenda for the Faculty Senate Meeting, March 27, 2025 (Held in MSC BE5)
    a. Approval of Proposed Agenda
    b. Approval of Minutes
    c. Announcements – Chair
    d. Guest Speaker: Susan Tusing
    e. Shared Governance Review Committee - Election
    f. Recommendations/Resolutions
    g. Regular Reports
        i. President – Brad Smith (15 minutes)
        ii. Provost – Avinandan Mukherjee (15 minutes)
        iii. Board of Governors – Robin Riner (5 minutes)
        iv. Advisory Council of Faculty – Amine Oudghiri-Otmani (5 minutes)
        v. Graduate Council – Richard Egleton (5 minutes)
        vi. Student Government Association – Brea Belville (5 minutes)
    h. Standing Committee Liaison Reports
        i. Academic Planning Committee – Daniel O'Malley (4 minutes)
        ii. Athletic Committee – Tom Hisiro (4 minutes)
        iii. Budget & Academic Policy Committee – Jana Tigchelaar (4 minutes)
        iv. Library Committee – Margie Phillips (4 minutes)
        v. Faculty Development Committee – Chair/Liaison (4 minutes)
        vi. Physical Facilities & Planning Committee – Jamey Halleck (4 minutes)
    i. Other Requests to Speak

Marshall University Faculty Senate
Executive Committee Minutes
Monday, February 10, 2025, 12:00 Noon
MSC 2W16b/Microsoft Teams

MEMBERS PRESENT: Nathaniel Ramsey (v), Heather Stark, Ross Salary, Uyi Lawani, Mike Huesmann, Zach Garrett, Shawn Schulenberg, Rick Gage, Jessica Buerk (v), Mindy Varney, Kelli Johnson, Amine Oudghiri-Otmani, Richard Egleton

MEMBERS ABSENT: None

EX-OFFICIO, NON-VOTING MEMBERS PRESENT: Robin Riner, Allison Carey, Brea Belville (v),

EX-OFFICIO, NON-VOTING MEMBERS ABSENT: None

PARLIAMENTARIAN: Zelideth Rivas

GUESTS: Carl Mummert, Karen McComas, Andrew Morelock, Anna Mummert, Jim Denvir, Teresa Eagle (v), Sonja Cantrell-Johnson (v), Eric Blough (v)

The meeting was convened at noon by Chair Shawn Schulenberg. Chair Schulenberg reviewed meeting procedures and expectations.

1. Approval of Proposed Agenda - approved

2. Approval of Minutes of January 13, 2025 - approved

3. Announcements – Chair

    1. The President has signed the following documents:
        a. November 11 Executive Committee Meeting Minutes
        b. November 21 Faculty Senate Meeting Minutes
        c. All Senate Recommendations/Resolutions, except for program reviews (07, 08, and 09), which always come later in the year.
    2. Just this morning, Physical Plant finalized a new home for our Faculty Award plaques. As you may remember, Kelli Johnson informed me in the fall that we had these plaques, unbeknownst to me, located on the 4th Floor of Drinko Library, and they had not been updated since 2016. Hailey Bibbee, our Office Administrator, has been working hard to update all plaques, including adding a new one for the Rucker Award. Thank you to Kelli and Hailey for your work, and I think they made a nice addition to the hallway immediately outside of the Senate Office in Old Main 310.
    3. The Board of Governors met last week and approved the Shared Governance Charter. The Senate is now tasked to elect its representative to the Shared Governance Review Committee. The Senate office will send out a call for nominations and we will hold an election at our March 27 Senate meeting.
    4. The Faculty Personnel Committee held an open forum on revisions to our Tenure and Promotion Policy (MU BOG AA 6, 7, and 9) and will integrate this feedback into a draft to consider before the end of this academic year.

5. The Ad Hoc Post Tenure Review Committee met last week, and it was a productive conversation. The committee's work is far from over and they are integrating the feedback into their current draft.

6. The Budget Advisory Committee will meet this afternoon at 1PM. The agenda includes review of support unit allocations, service level agreements, and key considerations for the proposal we are to send to the Executive Budget Committee, in addition to hearing feedback from the President and Deans.

7. This past week, a student was struck by a vehicle and injured on 3rd Avenue, near the same site where Maribeth Cox lost her life a little over three years ago. Since that incident, a handful of other students have also been injured in crosswalks around campus. Professor Jim Denvir has asked to say a few words and introduce a conversation on the topic at our February 20 Senate meeting, which I have placed on the proposed agenda. I have invited representatives from the administration to attend too, should we approve this as an agenda item later in this meeting.

8. Since we last met, new administrations have been inaugurated in both Charleston and Washington DC, and both have issued numerous executive orders possibly cutting both our research funding and implementing restrictions on diversity, equity, and inclusion. Regarding federal grant funding, the Trump administration proposed a broad federal freeze that was paused in the courts before the order was rescinded. Today, a new proposal is scheduled to go into effect that would restrict NIH indirect cost funding which covers things like equipment, operations, maintenance, accounting and personnel, is scheduled to go into effect today, to just 15 percent. Universities are bracing for the impact on their budget, as places like the University of Michigan announced that their current negotiated rate cap is 56%. I have not heard anything yet about what the impact will be on Marshall, but hopefully we will know more soon. In addition to these funding changes, both the federal government and the state have implemented new executive orders on diversity, equity, and inclusion, but the EOs are very vaguely worded, and our administration is currently searching for more clarity from Charleston. My own personal advice to faculty and chairs is this: do not proactively make any changes at the university, especially in the areas of teaching and research, until we have more guidance from university administration. I know this period of uncertainty is nerve racking for all.

9. The West Virginia Legislature begins its 60-day session this Wednesday, February 12. At the last Faculty Senate meeting, Dr. Marybeth Beller, our Faculty Senate liaison and the chair of the Legislative Affairs Committee, showed us how to track legislation on the legislature's website. She also discussed the potential impact of HR1, which would significantly change the legislative process. I encourage you to read up on this and reach out to your elected officials. Marshall Day at the WV State Capitol is scheduled for March 4. Please put it on your calendar and attend if possible. The format this year will focus on the six pillars, and we should hear more information about that soon.

10. Upcoming Meetings/Events

    a. The Spring General Faculty meeting is scheduled for April 10th, 2025, at 4:00 PM in the Joan C. Edwards Playhouse. Agenda items include honoring retiring faculty and the recognition of award-winning faculty.

    b. The items we consider today will be reviewed at our Faculty Senate meeting on February 20. Assistant Chair Varney will be the presiding officer.

    c. Our next Executive Committee meeting is scheduled for March 10 for items to be taken up at the March 27 Faculty Senate meeting. All recommendations and resolutions for those meetings are due at senate@marshall.edu by February 28.

4. Recommendations/Resolutions

    a. **SR 24-25-18 LAC** Recommends that the West Virginia State Legislature preserve and protect the seven Governor's Schools by ensuring that funding needs for each school are met. - approved

    b. **SR 24-25-19 CC** Recommends approval of the listed UNDERGRADUATE PROGRAM ADDITION, DELETION, CHANGE in the following college and/or schools/programs: Community Health; Social Work in Healthcare; BA Biological Sciences Degree; BA Biological Sciences Major; Music Education PreK-Adult; BA Criminal Justice; Corrections; Law Enforcement; Legal Studies; BS Pharmaceutical Sciences. -approved

    c. **SR 24-25-20 CC** Recommends approval of the listed UNDERGRADUATE COURSE ADDITION, DELETION, CHANGE in the following college and/or schools/programs: BUSN 280; ESS 450; SCLA 101H; SCLA 150; ANT 362; GEO 101; GEO 223; HST 428; PSC 200; PSC 304; PSC 499; CJ 322. - approved

Entered executive session at 12:11 p.m.

Exited executive session at 12:21 p.m.

    d. **SR 24-25-21 EC** Confidential Recommendation for Spring Commencement Speaker. - approved

    e. **SR 24-25-22 EC** Confidential Recommendation for Spring Honorary Degree Recipient(s). - approved

5. Set Agenda for the Faculty Senate Meeting, February 20, 2025 - approved

    a. Approval of Proposed Agenda

    b. Approval of Minutes

    c. Announcements – Chair

    d. Guest Speaker: Geoffrey Sheils (MU Board of Governors)

e. Recommendations/Resolutions

f. Regular Reports

i. President – Brad Smith (15 minutes)

ii. Provost – Avinandan Mukherjee (15 minutes)

iii. Board of Governors – Robin Riner (5 minutes)

iv. Advisory Council of Faculty – Amine Oudghiri-Otmani (5 minutes)

v. Graduate Council – Richard Egleton (5 minutes)

vi. Student Government Association – Brea Belville (5 minutes)

g. Standing Committee Liaison Reports

i. Legislative Affairs Committee – Marybeth Beller (4 minutes)

ii. University Curriculum Committee – Tim Melvin (4 minutes)

iii. Faculty Personnel Committee – Chair/Liaison (4 minutes)

iv. Research Committee – Philippe Georgel (4 minutes)

v. Student Conduct & Welfare Committee – Anthony Viola (4 minutes)

vi. Faculty Technology Committee – Nitin Puri (4 minutes)

h. Campus Safety – Jim Denvir (15 minutes)

i. Other Requests to Speak

The meeting was adjourned 12:22 p.m.

Respectfully Submitted:

Kelli Johnson

_____

Kelli Johnson, Recording Secretary
Faculty Senate

Marshall University Faculty Senate
Executive Committee Minutes
Monday, February 10, 2025, 12:00 Noon
MSC 2W16b/Microsoft Teams

MINUTES APPROVED BY EXECUTIVE COMMITTEE:

_____ _____

Shawn Schulenberg, Chair
Faculty Senate

Date Signed

MINUTES READ:

_____ _____

Brad Smith, President
Marshall University

Date Signed

BUDGET AND ACADEMIC POLICY COMMITTEE RECOMMENDATION

SR 24-25-23 BAPC

Recommends that Policy UPAA-2 ("Class Attendance") be revised as in the attached document.

It is further recommended that, in light of increased enrollment and the commensurate increase in requests for excused absences, additional resources be made available to Student Affairs in order to process these requests.

RATIONALE:

In the 2023-24 academic year, the Office of Student Advocacy and Accountability received over 3,000 requests for excused absences, placing a very large burden on their resources. To date, since the beginning of the 2024-2025 academic year, over 3,600 requests for excused absences have been processed. Many of these requests accumulate towards the end of the semester as students become aware of absences affecting their grade. The recommended changes represent an attempt to partially alleviate this burden, firstly by emphasizing that attendance policy can be handled on a course-by-course basis by the course instructor, and secondly by imposing a time limit on when students can request changes. We also recommend making further resources available to the Office of Student Advocacy and Accountability to address this issue.

Other changes are recommended:

- As many of our students come from non-traditional family backgrounds, we are recommending removing all language defining familial relationships in policy on absences related to critical illness and death.
- We also clarify that routine doctors' appointments scheduled in advance are not covered by this policy and are to be addressed solely between the student and instructor.
- Clarification is made that these policies apply to all classes with specific meeting times and assignments with specific due dates, regardless of the mode of delivery.
- The undergraduate catalog description of university excused absences includes a category for "extreme personal emergencies" which was not included in UPAA-2. We recommend adding this category to UPAA-2 to bring these documents in agreement.

BUDGET AND ACADEMIC POLICY COMMITTEE RECOMMENDATION

SR 24-25-23 BAPC
FACULTY SENATE CHAIR:

APPROVED BY THE
FACULTY SENATE: _____ DATE: _____

DISAPPROVED BY THE
FACULTY SENATE: _____ DATE: _____

UNIVERSITY PRESIDENT:

APPROVED: _____ DATE: _____

DISAPPROVED: _____ DATE: _____

COMMENTS: _____

_____

_____

_____

UNIVERSITY POLICY FOR ACADEMIC AFFAIRS

Policy No. UPAA-2

CLASS ATTENDANCE

1 General Information.

1.1 Scope: Academic policy regarding class attendance.

1.2 Authority: W. Va. Code §18B-1-6

1.3 Passage Date: September 12, 2019

1.4 Effective Date: October 15, 2019

1.5 Controlling over: Marshall University

1.6 History: Adopted General Faculty Meeting, May 12, 1970; Clarified by Faculty Senate on April 10, 2001; SR-04-05-(06)63 BAPC, Approved November 18, 2004 for Implementation Fall 2005. This version of the policy replaces an earlier version that was passed on March 8, 2006.

2 Policy

2.1 It is Marshall University's policy that each instructor evaluates the importance of student class attendance. In the course syllabus, the instructor must provide his/her policy on class attendance, make-up work, and related matters. If a student is absent from class because of a circumstance that is included in the excused absence policy, the absence can be handled by an arrangement between the student and the instructor or, if either party requests, the student can obtain an official excused absence following the procedure described below. The instructor must honor a university excused absence covered by this policy and allow the student an opportunity to catch up/make up work missed. This policy excludes those academic endeavors that require the completion of a certain number of clock hours, as in clinical experiences, practica or internships. For those courses, the maximum number of absences will be determined by the department chair or program supervisor. This policy does not supersede program accreditation requirements.

3 Definitions of Excused Absences

3.1 Excused absences fall into five categories:

3.1.1 University-sponsored activities

3.1.1.1 Academic activities including, but not limited to, performing arts, debate and individual events, honors classes, ROTC, and departmental functions.

3.1.1.2 Athletics, official athletic events sponsored by the Athletic Department.

3.1.1.3 Other University activities, including student government and student organizations.

The activity must have a clear educational mission and be closely linked to academic pursuits or to other official University functions.

3.1.2 Student Illness or Critical Illness/Death in the Immediate Family

3.1.2.1 “Immediate Family” is defined as a spouse/life partner, child, parent, legal guardian, sibling, grandparent or grandchild.

3.1.2.2 Student Illness or injury

3.1.2.2.1 Absences will be excused only for illnesses or injuries that prohibit students from participating in class.

3.1.2.3 Critical Illness of Immediate Family Member

3.1.2.3.1 Absences will be excused if the student documents that he or she had to provide needed care and/or support for a critically ill immediate family member.

3.1.2.4 Death of an Immediate Family Member

3.1.3 Short-Term Military Obligation: This is defined as absence as the result of military orders for a short-term period. Note: Students subject to federal activation are covered by a separate policy. Please see the catalog for this policy.

3.1.4 Jury Duty or Subpoena for Court Appearance

3.1.4.1 This applies to absences that are a result of official requests from a court of law.

3.1.5 Religious Holidays

3.1.5.1 This applies to major religious holidays. Please see the Office of Student Affairs for a list of such holidays.

4 Process

4.1 The student who seeks an excused absence must do so immediately after the event/activity/incident by following these guidelines. Whenever time permits, such as for University activities scheduled well in advance, the excuse must be obtained and presented to the instructor prior to the absence.

4.1.1 University Sponsored Activities

4.1.1.1 Academic Activities: These absences are excused by the dean within whose unit the activity is sponsored. The dean must pre-approve any notice that is given or sent to faculty regarding absences of this type.

4.1.1.2 Athletics: These absences are excused by the Chief Academic Officer (CAO), who must pre- approve any notice given/sent to faculty.

4.1.1.3 Other University activities: These absences are pre-approved by the Vice President of Student Affairs and excused by the Office of Academic Affairs prior to any notice to faculty. The activity and the excused absence must be endorsed in writing by the organization's advisor.

4.1.2 Student Illness or Critical Illness/Death in the Immediate Family

4.1.2.1 Student Illness or Injury: The student must submit official documentation of treatment by a medical practitioner to the Office of Student Affairs as soon as he/she returns to class. Documentation must specify the inclusive dates to be excused. The office will notify faculty that the absence(s) meets the criteria to be excused.

4.1.2.2 Critical Illness of Immediate Family Member: The student must submit official documentation from the family member's health care provider that substantiates the critical nature of the illness and the student's need to provide the care/support. This documentation is to be submitted to the of Student Affairs upon the student's return to class. The Office will notify faculty that the absence(s) meets the criteria to be excused.

4.1.2.3 Death of an Immediate Family Member: To obtain an excused absence, the student must submit one of the following to the Office of Student Affairs upon return to classes: an obituary or a funeral program with the student named as a relative; verification on letterhead stationery of the death and the relationship by clergy or funeral home personnel. The Office will notify faculty that the absence meets the criteria to be excused.

4.1.3 Short-Term Military Obligation

4.1.3.1 The student who seeks an excused absence for military obligation must present official documentation of his/her orders to duty to the dean of his/her college prior to the absence. The dean will notify faculty that the absences are to be excused.

4.1.4 Jury Duty or Subpoena for Court Appearance

4.1.4.1 The student who seeks an excused absence for jury duty or court appearance must submit his/her subpoena or official notification of jury duty to the dean of his/her college prior to the date of the obligation. The dean will notify faculty that the absence is to be excused.

4.1.5 Religious Holidays

4.1.5.1 Absences resulting from major religious holidays will be excused when the student presents the request in advance of the absence to the Office of Student Affairs. The dean will indicate his/her approval on the request and forward it to the Office of Academic Affairs for the official excused absence notification to faculty.

Notice: Any student who falsifies information or documentation in order to obtain an excused absence has committed a violation of the Code of Student Rights and Responsibilities and will be referred to Student Conduct for appropriate sanctions.

5 To Catch Up/Make Up Missed Work

5.1 It is the responsibility of the student to request an opportunity to complete missed work.

5.1.1 Once the excused absence has been secured, the request to make up work should immediately be made to the instructor at the next available class meeting.

5.1.2 Missed activities will be rescheduled or, in the event that rescheduling of an activity is not practical or possible, a fair and equitable alternative way of arriving at the grade for the missed component of the overall grade will be developed by the instructor.

5.1.3 Punitive measures must not be taken against students who present an official University excused absence.

5.1.4 Students should be aware that excessive absences—whether excused or unexcused—may affect their ability to earn a passing grade.

5.1.5 If the faculty member believes that the number of absences accrued under the terms of this policy is such that the student cannot fulfill the learning experience/mastery that a course requires, he/she may recommend that a student withdraw from the class.

5.1.6 Regardless of the nature of the excused absence, the student is responsible for completing all coursework prior to the end of the semester.

UNIVERSITY POLICY FOR ACADEMIC AFFAIRS
Policy No. UPAA-2
CLASS ATTENDANCE

2. Policy

2.1 It is Marshall University's policy that each instructor evaluates the importance of student class attendance. In the course syllabus, the instructor must provide his/her policy on class attendance, make-up work, and related matters. Reasons for excused absences are at the instructor's discretion but must include all excused absences listed in this policy, and the syllabus must include these excused absences either directly or by reference to this policy. If a student is absent from class because of a circumstance that is included in the class excused absence policy, the absence ~~can~~ will be ~~be~~ handled by an arrangement between the student and the instructor. In cases where a student has an absence whose excuse is guaranteed by this policy, and for which ~~or, if either party requests,~~ the instructor has not excused the student, the student can obtain an official excused absence following the procedure described below. ~~The instructor must honor a university excused absence covered by this policy and allow the student an opportunity to catch up/make up work missed.~~ This policy excludes those academic endeavors that require the completion of a certain number of clock hours, as in clinical experiences, practica or internships. For those courses, the maximum number of absences will be determined by the department chair or program supervisor. This policy covers all classes for which attendance is required at specific times by the course syllabus, and absences which affect the student's ability to submit assignments by a due date given in the syllabus. This policy does not supersede program accreditation requirements.

3. Definitions of Excused Absences

3.1 Excused absences fall into five categories:

3.1.1 University-sponsored activities

3.1.1.1 Academic activities including, but not limited to, performing arts, debate and individual events, honors classes, ROTC, and departmental functions.

3.1.1.2 Athletics, official athletic events sponsored by the Athletic Department.

3.1.1.3 Other University activities, including student government, academically-oriented ~~and~~ student organizations, and careers fairs. The activity must have a clear educational mission and be closely linked to academic pursuits or to other official University functions.

3.1.2 Student Illness or Critical Illness/Death of someone in a close relationship to the student.~~in the Immediate Family~~

~~3.1.2.1 "Immediate Family" is defined as a spouse/life partner, child, parent, legal guardian, sibling, grandparent or grandchild.~~

3.1.2.2 Student Illness or injury

3.1.2.2.1 Absences will be excused only for illnesses or injuries that prohibit students from participating in class. Routine doctor's appointments scheduled in advance are not considered excused absences in the scope of this policy and will not be approved by Student Affairs. (These may be approved as absences if agreed between the student and instructor.)

3.1.2.3 Critical Illness of someone in a close relationship to the student.~~Immediate Family Member~~

3.1.2.3.1 Absences will be excused if the student documents that he or she had to provide needed care and/or support for a critically ill ~~immediate~~ person~~family member~~.

3.1.2.4 Death of a~~n Immediate~~someone in a close relationship to the student.~~ Family Member~~

3.1.3 Short-Term Military Obligation: This is defined as absence as the result of military orders for a short-term period. Note: Students subject to federal activation are covered by a separate policy. Please see the catalog for this policy.

3.1.4 Jury Duty or Subpoena for Court Appearance

3.1.4.1 This applies to absences that are a result of official requests from a court of law.

3.1.5 Religious Holidays

3.1.5.1 This applies to major religious holidays. Please see the Office of Student Affairs for a list of such holidays.

3.1.6 Extreme personal emergencies.

3.1.6.1 Examples of such events include house fires, serious crimes, and other grave emergencies deemed by the Assistant Dean of Advocacy and Support to warrant an excused absence.

4 Process

4.1 Students should generally request an absence first from their instructor, within five instructional days ~~The student who seeks an excused absence must do so immediately~~ of the end of the event necessitating the absence. (For example, if a student is hospitalized, within one week of release from hospital.) ~~after the event/activity/incident by following these guidelines. Whenever time permits,~~For events that are scheduled in advance, such as ~~for~~ University activities, the excuse must be ~~obtained and presented to the~~requested from the instructor prior to the absence. Should the student receive a denial of the request for an excused absence, or should the

instructor not respond within five instructional days, the student may then request a university-excused absence as detailed below. The request for this absence must be made within five instructional days of the response from the instructor (or within 10 instructional days of the initial request to the instructor, in cases in which the instructor does not respond).

4.1.1 University Sponsored Activities

4.1.1.1 Academic Activities: These absences are excused by the dean within whose unit the activity is sponsored. The dean must pre-approve any notice that is given or sent to faculty regarding absences of this type.

4.1.1.2 Athletics: These absences are excused by the Chief Academic Officer (CAO), who must pre- approve any notice given/sent to faculty.

4.1.1.3 Other University activities: These absences are pre-approved by the Vice President of Student Affairs and excused by the Office of Academic Affairs prior to any notice to faculty. The activity and the excused absence must be endorsed in writing by the organization's advisor.

4.1.2 Student Illness or Critical Illness/Death of someone in a close relationship to the student~~in the Immediate Family~~

4.1.2.1 Student Illness or Injury: The student must submit official documentation of treatment by a medical practitioner to the Office of Student Affairs as soon as he/she returns to class. Documentation must specify the inclusive dates to be excused. The office will notify faculty that the absence(s) meets the criteria to be excused.

4.1.2.2 Critical Illness of someone in a close relationship to the student~~Immediate Family Member~~: The student must submit official documentation from the person~~family member~~'s health care provider that substantiates the critical nature of the illness and the student's need to provide the care/support. This documentation is to be submitted to the of Student Affairs upon the student's return to class. The Office will notify faculty that the absence(s) meets the criteria to be excused.

4.1.2.3 Death of someone in a close relationship to the student~~an Immediate Family Member~~: To obtain an excused absence, the student must submit one of the following to the Office of Student Affairs upon return to classes: an obituary or a funeral program~~ with the student named as a relative~~; verification on letterhead stationery of the death ~~and the relationship~~ by clergy or funeral home personnel. The student must also submit evidence of the relationship to the deceased. The Office will notify faculty that the absence meets the criteria to be excused.

4.1.3 Short-Term Military Obligation

4.1.3.1 The student who seeks an excused absence for military obligation must present official documentation of his/her orders to duty to the dean of his/her college prior to the absence. The dean will notify faculty that the absences are to be excused.

4.1.4 Jury Duty or Subpoena for Court Appearance

4.1.4.1 The student who seeks an excused absence for jury duty or court appearance must submit his/her subpoena or official notification of jury duty to the dean of his/her college prior to the date of the obligation. The dean will notify faculty that the absence is to be excused.

4.1.5 Religious Holidays

4.1.5.1 Absences resulting from major religious holidays will be excused when the student presents the request in advance of the absence to the Office of Student Affairs. The dean will indicate his/her approval on the request and forward it to the Office of Academic Affairs for the official excused absence notification to faculty.

Notice: Any student who falsifies information or documentation in order to obtain an excused absence has committed a violation of the Code of Student Rights and Responsibilities and will be referred to Student Conduct for appropriate sanctions.

Formatted: Indent: Left: 0", First line: 0"

UNIVERSITY POLICY FOR ACADEMIC AFFAIRS
Policy No. UPAA-2
CLASS ATTENDANCE

2. Policy

2.1 It is Marshall University's policy that each instructor evaluates the importance of student class attendance. In the course syllabus, the instructor must provide his/her policy on class attendance, make-up work, and related matters. Reasons for excused absences are at the instructor's discretion but must include all excused absences listed in this policy, and the syllabus must include these excused absences either directly or by reference to this policy. If a student is absent from class because of a circumstance that is included in the class excused absence policy, the absence will be handled by an arrangement between the student and the instructor. In cases where a student has an absence whose excuse is guaranteed by this policy, and for which the instructor has not excused the student, the student can obtain an official excused absence following the procedure described below. This policy excludes those academic endeavors that require the completion of a certain number of clock hours, as in clinical experiences, practica or internships. For those courses, the maximum number of absences will be determined by the department chair or program supervisor. This policy covers all classes for which attendance is required at specific times by the course syllabus, and absences which affect the student's ability to submit assignments by a due date given in the syllabus. This policy does not supersede program accreditation requirements.

3. Definitions of Excused Absences

3.1 Excused absences fall into five categories:

3.1.1 University-sponsored activities

3.1.1.1 Academic activities including, but not limited to, performing arts, debate and individual events, honors classes, ROTC, and departmental functions.

3.1.1.2 Athletics, official athletic events sponsored by the Athletic Department.

3.1.1.3 Other University activities, including student government, academically-oriented student organizations, and careers fairs. The activity must have a clear educational mission and be closely linked to academic pursuits or to other official University functions.

3.1.2 Student Illness or Critical Illness/Death of someone in a close relationship to the student.

3.1.2.2 Student Illness or injury

3.1.2.2.1 Absences will be excused only for illnesses or injuries that prohibit students from participating in class. Routine doctor's appointments scheduled in

advance are not considered excused absences in the scope of this policy and will not be approved by Student Affairs. (These may be approved as absences if agreed between the student and instructor.)

3.1.2.3 Critical Illness of someone in a close relationship to the student.

3.1.2.3.1 Absences will be excused if the student documents that he or she had to provide needed care and/or support for a critically ill person.

3.1.2.4 Death of a someone in a close relationship to the student.

3.1.3 Short-Term Military Obligation: This is defined as absence as the result of military orders for a short-term period. Note: Students subject to federal activation are covered by a separate policy. Please see the catalog for this policy.

3.1.4 Jury Duty or Subpoena for Court Appearance

3.1.4.1 This applies to absences that are a result of official requests from a court of law.

3.1.5 Religious Holidays

3.1.5.1 This applies to major religious holidays. Please see the Office of Student Affairs for a list of such holidays.

3.1.6 Extreme personal emergencies.

3.1.6.1 Examples of such events include house fires, serious crimes, and other grave emergencies deemed by the Assistant Dean of Advocacy and Support to warrant an excused absence.

4 Process

4.1 Students should generally request an absence first from their instructor, within five instructional days of the end of the event necessitating the absence. (For example, if a student is hospitalized, within one week of release from hospital.) For events that are scheduled in advance, such as University activities, the excuse must be requested from the instructor prior to the absence. Should the student receive a denial of the request for an excused absence, or should the instructor not respond within five instructional days, the student may then request a university-excused absence as detailed below. The request for this absence must be made within five instructional days of the response from the instructor (or within 10 instructional days of the initial request to the instructor, in cases in which the instructor does not respond).

4.1.1 University Sponsored Activities

4.1.1.1 Academic Activities: These absences are excused by the dean within whose unit the activity is sponsored. The dean must pre-approve any notice that is given or sent to faculty regarding absences of this type.

4.1.1.2 Athletics: These absences are excused by the Chief Academic Officer (CAO), who must pre- approve any notice given/sent to faculty.

4.1.1.3 Other University activities: These absences are pre-approved by the Vice President of Student Affairs and excused by the Office of Academic Affairs prior to any notice to faculty. The activity and the excused absence must be endorsed in writing by the organization's advisor.

4.1.2 Student Illness or Critical Illness/Death of someone in a close relationship to the student

4.1.2.1 Student Illness or Injury: The student must submit official documentation of treatment by a medical practitioner to the Office of Student Affairs as soon as he/she returns to class. Documentation must specify the inclusive dates to be excused. The office will notify faculty that the absence(s) meets the criteria to be excused.

4.1.2.2 Critical Illness of someone in a close relationship to the student: The student must submit official documentation from the person's health care provider that substantiates the critical nature of the illness and the student's need to provide the care/support. This documentation is to be submitted to the of Student Affairs upon the student's return to class. The Office will notify faculty that the absence(s) meets the criteria to be excused.

4.1.2.3 Death of someone in a close relationship to the student: To obtain an excused absence, the student must submit one of the following to the Office of Student Affairs upon return to classes: an obituary or a funeral program; verification on letterhead stationery of the death by clergy or funeral home personnel. The student must also submit evidence of the relationship to the deceased. The Office will notify faculty that the absence meets the criteria to be excused.

4.1.3 Short-Term Military Obligation

4.1.3.1 The student who seeks an excused absence for military obligation must present official documentation of his/her orders to duty to the dean of his/her college prior to the absence. The dean will notify faculty that the absences are to be excused.

4.1.4 Jury Duty or Subpoena for Court Appearance

4.1.4.1 The student who seeks an excused absence for jury duty or court appearance must submit his/her subpoena or official notification of jury duty to the dean of his/her college prior to the date of the obligation. The dean will notify faculty that the absence is to be excused.

4.1.5 Religious Holidays

4.1.5.1 Absences resulting from major religious holidays will be excused when the student presents the request in advance of the absence to the Office of Student Affairs. The dean will indicate his/her approval on the request and forward it to the Office of Academic Affairs for the official excused absence notification to faculty.

Notice: Any student who falsifies information or documentation in order to obtain an excused absence has committed a violation of the Code of Student Rights and Responsibilities and will be referred to Student Conduct for appropriate sanctions.

BUDGET AND ACADEMIC POLICY COMMITTEE RECOMMENDATION

SR 24-25-24 BAPC

Recommends that Policy UPGA-2 ("Policy regarding weather-related and/or emergency closings and delays") be amended as in the attached document.

RATIONALE:

The university excused absence policy (UPAA-2) does not provide a provision for excusing absences for commuting students who are unable to safely attend class due to adverse weather conditions. The decision for mandating excuses for such absences is subjective, and as such is not best determined on a course-by-course basis by individual instructors. The recommended revisions to this policy allow those responsible for decisions on weather-related closures (the Chief of Staff, the Senior Vice President for Academic Affairs, and the Senior Vice President for Operations) to mandate instructors excuse absences for inclement weather that may prohibit safe commuting to campus but which is not severe enough to close or delay university operations.

FACULTY SENATE CHAIR:

APPROVED BY THE
FACULTY SENATE: _____ DATE: _____

DISAPPROVED BY THE
FACULTY SENATE: _____ DATE: _____

UNIVERSITY PRESIDENT:

APPROVED: _____ DATE: _____

DISAPPROVED: _____ DATE: _____

COMMENTS: _____

_____

_____

_____

UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

Policy No. UPGA-2

POLICY REGARDING WEATHER-RELATED AND/OR EMERGENCY CLOSINGS AND DELAYS

1 General Information.

1.1 Scope: This policy describes notification procedures and student and employee attendance expectations in the event of a delay or closing of the institutions.

1.2 Authority: W. Va. Code §18B-1-6

1.3 Passage Date: June 28, 2019

1.4 Effective Date: August 1, 2019

1.5 Controlling over: Marshall University

1.6 History:

1.6.1 This policy amends GA-9 (effective June 11, 2019), which amended GA-9 (effective October 15, 2009), which amended GA-9 (effective March 8, 2006) which replaced Executive Policy Bulletin No. 7, (revised February 1, 2005). The amendments provide for a form of compensatory time for employees required to work during a closing.

2 Policy.

2.1 Generally, it is Marshall University's policy to maintain its normal schedule, even when conditions are inclement. However, that is not always possible.

3 Huntington Campus Delays and Closings.

3.1 In those instances when it is necessary to alter the schedule in response to weather conditions, every effort will be made to notify all those affected—students, faculty, staff and the general public—as expeditiously and as comprehensively as possible in the following ways:

3.1.1 The university subscribes to a third-party service to provide notifications by e-mail, text message, and telephone, referred to as "MU Alert" at Marshall. All students, faculty and staff will be enrolled in the MU Alert database with their university e-mail addresses, and, in the case of faculty and staff, their office telephone numbers. Students, faculty and staff may provide additional contact methods, including those for text messaging and cell phone numbers, through the use of the myMU portal.

In cases of weather-related or other emergency closings and delays, University Communications staff will use MU Alert to send notification.

3.1.2 Television stations in Huntington and Charleston will be notified.

3.1.3 Radio stations in Huntington and Charleston will be asked to announce the delay or closing.

3.1.4 Time permitting; newspapers in Huntington and Charleston will be notified. Often, however, decisions must be made after deadlines of newspapers.

3.1.5 The Office of University Communications will communicate the specific details of the delay or closing to the Office of Public Safety at 304-696-HELP.

3.1.6 Notifications will be posted on the University's official social media accounts.

3.2 Information about closing, cancellations, or delays will ordinarily be disseminated to area radio and television stations. The authoritatively correct statement of the University's condition (Huntington) is stipulated to be the message on the main page of the website at http://www.marshall.edu.

3.3 This section applies only to the Huntington campus and all releases should make it clear that it relates only to the Huntington campus. The chief administrative officer (as designated by the University president) will manage the weather-related closings policy for the South Charleston campus and other education centers for the respective location, and all releases should make clear that the release applies only to the affected location. The South Charleston phone number is 304-746-2500. See Section 4 for information on procedures for other locations.

3.4 Types of delays and closings**:**

3.4.1 University Closed: All classes suspended and offices closed.

3.4.2 Classes Cancelled: All classes suspended; offices open.

3.4.3 Delay Code A: Means a delay in the opening of classes BUT no delay in the opening of offices. Delays will usually be in the range of one to two hours. Employees are expected to report to work at their normal starting times unless they feel that travel is unsafe. If an employee feels that he/she cannot travel safely to work, he/she may charge accrued annual leave for the portion of the workday from 8:00 a.m. (or their normal start time) until their arrival at work.

3.4.4 Delay Code B: Means a delay in the opening of classes AND a delay in the opening of offices. Delays will usually be in the range of one to two hours. Employees do not have to report to their offices until the stated delay time. If they believe they cannot travel to work safely by the stated delay time, they may charge accrued annual leave for the work hours from the stated delay time until they can next report to work.

3.4.5 Class operation under delays: Under both categories of delay, students should go to the class that would begin at the stated delay time or the class that would have convened within 30 minutes of the stated delay time. A two-hour delay means that classes that begin at 10:00 a.m. begin on time. Classes that begin at 9:30 a.m. meet at 10:00 a.m. and continue for the remaining period of that class.

3.4.6 Exceptions with regard to employees: Certain critical and emergency employees may be required to report to work on time or earlier than normally scheduled despite the particular delay code published.

3.5 Staff and administrative personnel procedures:

3.5.1 The university will be completely closed only rarely and in extreme situations since it is essential that public safety be maintained, that buildings and equipment be protected and that services be provided for those students housed in campus facilities. Therefore, under Classes Cancelled, above, all university staff and administrative employees will be expected to report to work, unless notified otherwise.

3.5.2 In the event of critical need, certain employees may be required to report to work or temporarily reside on campus to ensure human safety and preservation of university property or facilities.

3.5.2.1 Employees may be eligible for substitute time off (STO) if they were directed by their supervisor to be present for work during a period of inclement weather closing or other emergency closing. Eligible individuals must be in regular-status, leave-accruing employment and must have received a direct instruction from their supervisor to be present for work during such a closing. Eligible part-time employees may receive STO on a pro rata basis according to appointed percentage time unless they actually worked longer than their appointed hours. The provision of STO for such periods of inclement weather/other emergency closing is authorized by the responsible vice president or his/her designee.

3.5.2.2 In order to provide STO to an eligible employee, the supervisor must produce a statement to be preserved in the employing department which will include (1) identification of the affected employee(s); (2) a statement that the employee(s) was/were directed by him/her to come to work or remain at work for any or all of a period of inclement weather/other emergency closing; and (3) a statement of why it was necessary to require the employee(s) to attend work. A copy of the statement(s) should be sent to Human Resource Services.

3.5.2.3 The following should be noted: (1) eligibility for STO is not determined on the basis of being a member of a work group or work unit deemed essential; (2) status as a federal Fair Labor Standards Act (FLSA) non-exempt or exempt employee does not apply because the periods of inclement weather/other emergency closing do not represent overtime; (3) no employee is eligible for STO who was present for work for some or all of the periods of inclement weather/other emergency closing on a voluntary or elective basis; (4) premium pay or premium compensatory time off for holidays worked does not apply because the inclement weather/other emergency closings are not holidays; (5) STO is not compensatory time off as used in calculations of Fair Labor Standards Act overtime for hours actually worked; (6) STO may be provided in cases where the employee was directed to report to work at a time prior to the determination of inclement weather/other emergency closing [such direction will be construed to mean a stated requirement to come to work just as if inclement weather/other emergency closing had actually been announced]; and (7) STO made available due to inclement weather or other emergency closing must be used within one year of its award.

3.5.2.4 Nothing in this process shall preclude a non-exempt employee from earning additional straight time or Fair Labor Standards Act (FLSA) overtime pay or compensatory time off for weeks which include emergency closing(s) and during which the subject employee worked more than 37.5 hours (with respect to additional straight time pay) or worked more than 40.0 hours (with respect to FLSA overtime pay or compensatory time off).

3.5.3 Individual employees may, in their best judgment, determine the risk of travel to be too great and elect to remain home. Those who do should contact their respective supervisors and indicate they are: (1) taking annual leave that day, or (2) taking compensatory time, in the event compensatory time is owed to them**.**

3.5.4 In the event a building, or section of a building is closed (because of heat loss, power outage, etc.) employees working in that affected area will be permitted to take their work to another area or building on campus. Or, in consultation with the supervisor, the employee may elect to take annual leave that day, or take compensatory time off.

3.5.5 In the event of an extreme situation (tornado, flood, ice storm, campus disturbance, etc.) and the employees' presence is not desired on campus, this information will be disseminated via MU Alert. A decision as to whether the missed time will be chargeable to annual leave, compensatory time, or a non-pay situation will be determined by the president and communicated through supervisors.

3.5.6 Supervisors must take steps to ensure offices and workstations are open to employees at all time when those employees are expected to be at work, including inclement weather situations and other disruptive situations.

3.6 Faculty:

3.6.1 Once operations are resumed, deans and departmental chairs must take steps to ensure that faculty meet their scheduled classes or substitutes secured so that class schedules are met.

3.7 Decision Making:

3.7.1 Decisions on closings and/or delays will be made jointly by the Chief of Staff, Senior Vice President for Academic Affairs and the Senior Vice President for Operations following the consultation with other appropriate officials, including the President. Should only one or two of those three persons be available, the ones available will make the decision.

3.7.2 Every effort will be made to reach decisions to allow time for adequate notification of those affected.

4 South Charleston campus and other education centers:

4.1 Because weather conditions can vary substantially, it is possible that classes will be delayed or cancelled at some locations and not at others. The chief administrative officer for each location, in consultation with local staff, will decide on class cancellations.

4.1.1 South Charleston campus: Notification of delays or cancellations at the South Charleston campus will be announced by (a) University website (b) MU Alert (c) University official Facebook and Twitter social accounts, and (d) local media. Students may check the status of their classes by checking the website.

4.1.2 Point Pleasant, Beckley, Teays Valley and other educational centers: Procedures for delayed openings and class cancellations are similar to those for the South Charleston campus. At Point Pleasant, Beckley, and Teays Valley, information regarding cancellations will be provided on the University website, and through MU Alert, the University's official Facebook and Twitter social media accounts, and local media.

4.1.3 Remote locations and other educational centers: Because there may be classes meeting on an irregular schedule in a geographically dispersed area throughout the semester, decisions about whether to meet during inclement weather will be made by the instructor. Those decisions will be transmitted to students by e-mail or other methods as agreed by students and the instructor.

4.2 Types of delays and closings for the South Charleston campus:

4.2.1 South Charleston Closed: All classes cancelled and offices closed.

4.2.2 South Charleston Classes Cancelled: All classes cancelled. Details provided by site.

4.2.3 South Charleston Delay: A delay in the beginning of non-class activities, e.g. a two-hour delay would mean the normal workday would begin at 10:00 a.m. rather than 8:00 a.m.

4.2.4

5 Marshall University School of Medicine

5.1 Due to the unique nature of its obligations to its constituents, the Marshall University School of Medicine may maintain a separate set of procedures for weather-related and emergency closings.

UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

Policy No. UPGA-2

POLICY REGARDING WEATHER-RELATED AND/OR EMERGENCY CLOSINGS AND DELAYS

1 General Information.

1.1 Scope: This policy describes notification procedures and student and employee attendance expectations in the event of a delay or closing of the institutions.

1.2 Authority: W. Va. Code §18B-1-6

1.3 Passage Date: ~~June 28, 2019~~

1.4 Effective Date: ~~August 1, 2019~~

1.5 Controlling over: Marshall University

1.6 History:

1.6.1 This policy amends GA-9 (effective August 1, 2019), which amended UPGA-2 (effective June 11, 2019), which amended GA-9 (effective October 15, 2009), which amended GA-9 (effective March 8, 2006) which replaced Executive Policy Bulletin No. 7, (revised February 1, 2005). The amendments provide for ~~a form of compensatory time for employees required to work during a closing.~~mandating excused absences in the event of inclement weather when the university operates under a normal schedule.

2 Policy.

2.1 Generally, it is Marshall University's policy to maintain its normal schedule, even when conditions are inclement. However, that is not always possible.

3 Huntington Campus Delays and Closings.

3.1 In those instances when it is necessary to alter the schedule in response to weather conditions, every effort will be made to notify all those affected—students, faculty, staff and the general public—as expeditiously and as comprehensively as possible in the following ways:

3.1.1 The university subscribes to a third-party service to provide notifications by e-mail, text message, and telephone, referred to as "MU Alert" at Marshall. All students, faculty and staff will be enrolled in the MU Alert database with their university e-mail addresses, and, in the case of faculty and staff, their office telephone numbers. Students, faculty and staff may provide additional contact methods, including those for text messaging and cell phone numbers, through the use of the myMU portal.

In cases of weather-related or other emergency closings and delays, University Communications staff will use MU Alert to send notification.

3.1.2 Television stations in Huntington and Charleston will be notified.

3.1.3 Radio stations in Huntington and Charleston will be asked to announce the delay or closing.

3.1.4 Time permitting; newspapers in Huntington and Charleston will be notified. Often, however, decisions must be made after deadlines of newspapers.

3.1.5 The Office of University Communications will communicate the specific details of the delay or closing to the Office of Public Safety at 304-696-HELP.
3.1.6 Notifications will be posted on the University's official social media accounts.

3.2 Information about closing, cancellations, or delays will ordinarily be disseminated to area radio and television stations. The authoritatively correct statement of the University's condition (Huntington) is stipulated to be the message on the main page of the website at http://www.marshall.edu.

3.3 This section applies only to the Huntington campus and all releases should make it clear that it relates only to the Huntington campus. The chief administrative officer (as designated by the University president) will manage the weather-related closings policy for the South Charleston campus and other education centers for the respective location, and all releases should make clear that the release applies only to the affected location. The South Charleston phone number is 304-746-2500. See Section 4 for information on procedures for other locations.

3.4 Types of delays and closings**:**
3.4.1 University Closed: All classes suspended and offices closed.
3.4.2 Classes Cancelled: All classes suspended; offices open.
3.4.3 Classes Non-Mandatory: Classes meet as normal and offices are open. Instructors are required to excuse absences to students in in-person classes who are unable to travel to the class.
3.4.4 Delay Code A: Means a delay in the opening of classes BUT no delay in the opening of offices. Delays will usually be in the range of one to two hours. Employees are expected to report to work at their normal starting times unless they feel that travel is unsafe. If an employee feels that he/she cannot travel safely to work, he/she may charge accrued annual leave for the portion of the workday from 8:00 a.m. (or their normal start time) until their arrival at work.
3.4.5 Delay Code B: Means a delay in the opening of classes AND a delay in the opening of offices. Delays will usually be in the range of one to two hours. Employees do not have to report to their offices until the stated delay time. If they believe they cannot travel to work safely by the stated delay time, they may charge accrued annual leave for the work hours from the stated delay time until they can next report to work.
3.4.6 Class operation under delays: Under both categories of delay, students should go to the class that would begin at the stated delay time or the class that would have convened within 30 minutes of the stated delay time. A two-hour delay means that classes that begin at 10:00 a.m. begin on time. Classes that begin at 9:30 a.m. meet at 10:00 a.m. and continue for the remaining period of that class.
3.4.7 Exceptions with regard to employees: Certain critical and emergency employees may be required to report to work on time or earlier than normally scheduled despite the particular delay code published.

3.5 Staff and administrative personnel procedures:
3.5.1 The university will be completely closed only rarely and in extreme situations since it is essential that public safety be maintained, that buildings and equipment be protected and that

services be provided for those students housed in campus facilities. Therefore, under Classes Cancelled, above, all university staff and administrative employees will be expected to report to work, unless notified otherwise.

3.5.2 In the event of critical need, certain employees may be required to report to work or temporarily reside on campus to ensure human safety and preservation of university property or facilities.

3.5.2.1 Employees may be eligible for substitute time off (STO) if they were directed by their supervisor to be present for work during a period of inclement weather closing or other emergency closing. Eligible individuals must be in regular-status, leave-accruing employment and must have received a direct instruction from their supervisor to be present for work during such a closing. Eligible part-time employees may receive STO on a pro rata basis according to appointed percentage time unless they actually worked longer than their appointed hours. The provision of STO for such periods of inclement weather/other emergency closing is authorized by the responsible vice president or his/her designee.

3.5.2.2 In order to provide STO to an eligible employee, the supervisor must produce a statement to be preserved in the employing department which will include (1) identification of the affected employee(s); (2) a statement that the employee(s) was/were directed by him/her to come to work or remain at work for any or all of a period of inclement weather/other emergency closing; and (3) a statement of why it was necessary to require the employee(s) to attend work. A copy of the statement(s) should be sent to Human Resource Services.

3.5.2.3 The following should be noted: (1) eligibility for STO is not determined on the basis of being a member of a work group or work unit deemed essential; (2) status as a federal Fair Labor Standards Act (FLSA) non-exempt or exempt employee does not apply because the periods of inclement weather/other emergency closing do not represent overtime; (3) no employee is eligible for STO who was present for work for some or all of the periods of inclement weather/other emergency closing on a voluntary or elective basis; (4) premium pay or premium compensatory time off for holidays worked does not apply because the inclement weather/other emergency closings are not holidays; (5) STO is not compensatory time off as used in calculations of Fair Labor Standards Act overtime for hours actually worked; (6) STO may be provided in cases where the employee was directed to report to work at a time prior to the determination of inclement weather/other emergency closing [such direction will be construed to mean a stated requirement to come to work just as if inclement weather/other emergency closing had actually been announced]; and (7) STO made available due to inclement weather or other emergency closing must be used within one year of its award.

3.5.2.4 Nothing in this process shall preclude a non-exempt employee from earning additional straight time or Fair Labor Standards Act (FLSA) overtime pay or compensatory time off for weeks which include emergency closing(s) and during which the subject employee worked more than 37.5 hours (with respect to additional straight time pay) or worked more than 40.0 hours (with respect to FLSA overtime pay or compensatory time off).

3.5.3 Individual employees may, in their best judgment, determine the risk of travel to be too great and elect to remain home. Those who do should contact their respective supervisors and indicate they are: (1) taking annual leave that day, or (2) taking compensatory time, in the event compensatory time is owed to them**.**

3.5.4 In the event a building, or section of a building is closed (because of heat loss, power outage, etc.) employees working in that affected area will be permitted to take their work to

another area or building on campus. Or, in consultation with the supervisor, the employee may elect to take annual leave that day, or take compensatory time off.

3.5.5 In the event of an extreme situation (tornado, flood, ice storm, campus disturbance, etc.) and the employees' presence is not desired on campus, this information will be disseminated via MU Alert. A decision as to whether the missed time will be chargeable to annual leave, compensatory time, or a non-pay situation will be determined by the president and communicated through supervisors.

3.5.6 Supervisors must take steps to ensure offices and workstations are open to employees at all time when those employees are expected to be at work, including inclement weather situations and other disruptive situations.

3.6 Faculty:
3.6.1 Once operations are resumed, deans and departmental chairs must take steps to ensure that faculty meet their scheduled classes or substitutes secured so that class schedules are met.

3.7 Decision Making:
3.7.1 Decisions on closings and/or delays will be made jointly by the Chief of Staff, Senior Vice President for Academic Affairs and the Senior Vice President for Operations following the consultation with other appropriate officials, including the President. Should only one or two of those three persons be available, the ones available will make the decision.
3.7.2 Every effort will be made to reach decisions to allow time for adequate notification of those affected.

4 South Charleston campus and other education centers:
4.1 Because weather conditions can vary substantially, it is possible that classes will be delayed or cancelled at some locations and not at others. The chief administrative officer for each location, in consultation with local staff, will decide on class cancellations.
4.1.1 South Charleston campus: Notification of delays or cancellations at the South Charleston campus will be announced by (a) University website (b) MU Alert (c) University official Facebook and Twitter social accounts, and (d) local media. Students may check the status of their classes by checking the website.
4.1.2 Point Pleasant, Beckley, Teays Valley and other educational centers: Procedures for delayed openings and class cancellations are similar to those for the South Charleston campus. At Point Pleasant, Beckley, and Teays Valley, information regarding cancellations will be provided on the University website, and through MU Alert, the University's official Facebook and Twitter social media accounts, and local media.
4.1.3 Remote locations and other educational centers: Because there may be classes meeting on an irregular schedule in a geographically dispersed area throughout the semester, decisions about whether to meet during inclement weather will be made by the instructor. Those decisions will be transmitted to students by e-mail or other methods as agreed by students and the instructor.

4.2 Types of delays and closings for the South Charleston campus:

4.2.1 South Charleston Closed: All classes cancelled and offices closed.
4.2.2 South Charleston Classes Cancelled: All classes cancelled. Details provided by site.
4.2.3 South Charleston Classes non-mandatory: Classes meet as normal. Instructors must excuse absences for students in in-person classes who are unable to travel to class.
4.2.4 South Charleston Delay: A delay in the beginning of non-class activities, e.g. a two-hour delay would mean the normal workday would begin at 10:00 a.m. rather than 8:00 a.m.

5 Marshall University School of Medicine

5.1 Due to the unique nature of its obligations to its constituents, the Marshall University School of Medicine may maintain a separate set of procedures for weather-related and emergency closings.

UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

Policy No. UPGA-2

POLICY REGARDING WEATHER-RELATED AND/OR EMERGENCY CLOSINGS AND DELAYS

1 General Information.

1.1 Scope: This policy describes notification procedures and student and employee attendance expectations in the event of a delay or closing of the institutions.

1.2 Authority: W. Va. Code §18B-1-6

1.3 Passage Date:

1.4 Effective Date:

1.5 Controlling over: Marshall University

1.6 History:

1.6.1 This policy amends GA-9 (effective August 1, 2019), which amended UPGA-2 (effective June 11, 2019), which amended GA-9 (effective October 15, 2009), which amended GA-9 (effective March 8, 2006) which replaced Executive Policy Bulletin No. 7, (revised February 1, 2005). The amendments provide for mandating excused absences in the event of inclement weather when the university operates under a normal schedule.

2 Policy.

2.1 Generally, it is Marshall University's policy to maintain its normal schedule, even when conditions are inclement. However, that is not always possible.

3 Huntington Campus Delays and Closings.

3.1 In those instances when it is necessary to alter the schedule in response to weather conditions, every effort will be made to notify all those affected—students, faculty, staff and the general public—as expeditiously and as comprehensively as possible in the following ways:

3.1.1 The university subscribes to a third-party service to provide notifications by e-mail, text message, and telephone, referred to as "MU Alert" at Marshall. All students, faculty and staff will be enrolled in the MU Alert database with their university e-mail addresses, and, in the case of faculty and staff, their office telephone numbers. Students, faculty and staff may provide additional contact methods, including those for text messaging and cell phone numbers, through the use of the myMU portal.

In cases of weather-related or other emergency closings and delays, University Communications staff will use MU Alert to send notification.

3.1.2 Television stations in Huntington and Charleston will be notified.

3.1.3 Radio stations in Huntington and Charleston will be asked to announce the delay or closing.

3.1.4 Time permitting; newspapers in Huntington and Charleston will be notified. Often, however, decisions must be made after deadlines of newspapers.

3.1.5 The Office of University Communications will communicate the specific details of the delay or closing to the Office of Public Safety at 304-696-HELP.
3.1.6 Notifications will be posted on the University's official social media accounts.

3.2 Information about closing, cancellations, or delays will ordinarily be disseminated to area radio and television stations. The authoritatively correct statement of the University's condition (Huntington) is stipulated to be the message on the main page of the website at http://www.marshall.edu.

3.3 This section applies only to the Huntington campus and all releases should make it clear that it relates only to the Huntington campus. The chief administrative officer (as designated by the University president) will manage the weather-related closings policy for the South Charleston campus and other education centers for the respective location, and all releases should make clear that the release applies only to the affected location. The South Charleston phone number is 304-746-2500. See Section 4 for information on procedures for other locations.

3.4 Types of delays and closings**:**
3.4.1 University Closed: All classes suspended and offices closed.
3.4.2 Classes Cancelled: All classes suspended; offices open.
3.4.3 Classes Non-Mandatory: Classes meet as normal and offices are open. Instructors are required to excuse absences to students in in-person classes who are unable to travel to the class.
3.4.4 Delay Code A: Means a delay in the opening of classes BUT no delay in the opening of offices. Delays will usually be in the range of one to two hours. Employees are expected to report to work at their normal starting times unless they feel that travel is unsafe. If an employee feels that he/she cannot travel safely to work, he/she may charge accrued annual leave for the portion of the workday from 8:00 a.m. (or their normal start time) until their arrival at work.
3.4.5 Delay Code B: Means a delay in the opening of classes AND a delay in the opening of offices. Delays will usually be in the range of one to two hours. Employees do not have to report to their offices until the stated delay time. If they believe they cannot travel to work safely by the stated delay time, they may charge accrued annual leave for the work hours from the stated delay time until they can next report to work.
3.4.6 Class operation under delays: Under both categories of delay, students should go to the class that would begin at the stated delay time or the class that would have convened within 30 minutes of the stated delay time. A two-hour delay means that classes that begin at 10:00 a.m. begin on time. Classes that begin at 9:30 a.m. meet at 10:00 a.m. and continue for the remaining period of that class.
3.4.7 Exceptions with regard to employees: Certain critical and emergency employees may be required to report to work on time or earlier than normally scheduled despite the particular delay code published.

3.5 Staff and administrative personnel procedures:
3.5.1 The university will be completely closed only rarely and in extreme situations since it is essential that public safety be maintained, that buildings and equipment be protected and that

services be provided for those students housed in campus facilities. Therefore, under Classes Cancelled, above, all university staff and administrative employees will be expected to report to work, unless notified otherwise.

3.5.2 In the event of critical need, certain employees may be required to report to work or temporarily reside on campus to ensure human safety and preservation of university property or facilities.

3.5.2.1 Employees may be eligible for substitute time off (STO) if they were directed by their supervisor to be present for work during a period of inclement weather closing or other emergency closing. Eligible individuals must be in regular-status, leave-accruing employment and must have received a direct instruction from their supervisor to be present for work during such a closing. Eligible part-time employees may receive STO on a pro rata basis according to appointed percentage time unless they actually worked longer than their appointed hours. The provision of STO for such periods of inclement weather/other emergency closing is authorized by the responsible vice president or his/her designee.

3.5.2.2 In order to provide STO to an eligible employee, the supervisor must produce a statement to be preserved in the employing department which will include (1) identification of the affected employee(s); (2) a statement that the employee(s) was/were directed by him/her to come to work or remain at work for any or all of a period of inclement weather/other emergency closing; and (3) a statement of why it was necessary to require the employee(s) to attend work. A copy of the statement(s) should be sent to Human Resource Services.

3.5.2.3 The following should be noted: (1) eligibility for STO is not determined on the basis of being a member of a work group or work unit deemed essential; (2) status as a federal Fair Labor Standards Act (FLSA) non-exempt or exempt employee does not apply because the periods of inclement weather/other emergency closing do not represent overtime; (3) no employee is eligible for STO who was present for work for some or all of the periods of inclement weather/other emergency closing on a voluntary or elective basis; (4) premium pay or premium compensatory time off for holidays worked does not apply because the inclement weather/other emergency closings are not holidays; (5) STO is not compensatory time off as used in calculations of Fair Labor Standards Act overtime for hours actually worked; (6) STO may be provided in cases where the employee was directed to report to work at a time prior to the determination of inclement weather/other emergency closing [such direction will be construed to mean a stated requirement to come to work just as if inclement weather/other emergency closing had actually been announced]; and (7) STO made available due to inclement weather or other emergency closing must be used within one year of its award.

3.5.2.4 Nothing in this process shall preclude a non-exempt employee from earning additional straight time or Fair Labor Standards Act (FLSA) overtime pay or compensatory time off for weeks which include emergency closing(s) and during which the subject employee worked more than 37.5 hours (with respect to additional straight time pay) or worked more than 40.0 hours (with respect to FLSA overtime pay or compensatory time off).

3.5.3 Individual employees may, in their best judgment, determine the risk of travel to be too great and elect to remain home. Those who do should contact their respective supervisors and indicate they are: (1) taking annual leave that day, or (2) taking compensatory time, in the event compensatory time is owed to them**.**

3.5.4 In the event a building, or section of a building is closed (because of heat loss, power outage, etc.) employees working in that affected area will be permitted to take their work to

another area or building on campus. Or, in consultation with the supervisor, the employee may elect to take annual leave that day, or take compensatory time off.

3.5.5 In the event of an extreme situation (tornado, flood, ice storm, campus disturbance, etc.) and the employees' presence is not desired on campus, this information will be disseminated via MU Alert. A decision as to whether the missed time will be chargeable to annual leave, compensatory time, or a non-pay situation will be determined by the president and communicated through supervisors.

3.5.6 Supervisors must take steps to ensure offices and workstations are open to employees at all time when those employees are expected to be at work, including inclement weather situations and other disruptive situations.

3.6 Faculty:
3.6.1 Once operations are resumed, deans and departmental chairs must take steps to ensure that faculty meet their scheduled classes or substitutes secured so that class schedules are met.

3.7 Decision Making:
3.7.1 Decisions on closings and/or delays will be made jointly by the Chief of Staff, Senior Vice President for Academic Affairs and the Senior Vice President for Operations following the consultation with other appropriate officials, including the President. Should only one or two of those three persons be available, the ones available will make the decision.
3.7.2 Every effort will be made to reach decisions to allow time for adequate notification of those affected.

4 South Charleston campus and other education centers:
4.1 Because weather conditions can vary substantially, it is possible that classes will be delayed or cancelled at some locations and not at others. The chief administrative officer for each location, in consultation with local staff, will decide on class cancellations.
4.1.1 South Charleston campus: Notification of delays or cancellations at the South Charleston campus will be announced by (a) University website (b) MU Alert (c) University official Facebook and Twitter social accounts, and (d) local media. Students may check the status of their classes by checking the website.
4.1.2 Point Pleasant, Beckley, Teays Valley and other educational centers: Procedures for delayed openings and class cancellations are similar to those for the South Charleston campus. At Point Pleasant, Beckley, and Teays Valley, information regarding cancellations will be provided on the University website, and through MU Alert, the University's official Facebook and Twitter social media accounts, and local media.
4.1.3 Remote locations and other educational centers: Because there may be classes meeting on an irregular schedule in a geographically dispersed area throughout the semester, decisions about whether to meet during inclement weather will be made by the instructor. Those decisions will be transmitted to students by e-mail or other methods as agreed by students and the instructor.

4.2 Types of delays and closings for the South Charleston campus:

4.2.1 South Charleston Closed: All classes cancelled and offices closed.
4.2.2 South Charleston Classes Cancelled: All classes cancelled. Details provided by site.
4.2.3 South Charleston Classes non-mandatory: Classes meet as normal. Instructors must excuse absences for students in in-person classes who are unable to travel to class.
4.2.4 South Charleston Delay: A delay in the beginning of non-class activities, e.g. a two-hour delay would mean the normal workday would begin at 10:00 a.m. rather than 8:00 a.m.

5 Marshall University School of Medicine

5.1 Due to the unique nature of its obligations to its constituents, the Marshall University School of Medicine may maintain a separate set of procedures for weather-related and emergency closings.

University Curriculum Committee
RECOMMENDATION

SR 24-25-25 CC Recommends approval of the listed **UNDERGRADUATE PROGRAM ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

INSTRUCTIONS: To view each full proposal (including all forms and attachments), log in to Courseleaf CIM using your MU credentials from the links below

- **All Proposals (by Approval Level)** https://nextcatalog.marshall.edu/courseleaf/approve/
  - Use this link to view **all proposals** (courses/programs/miscellaneous/intents-to-plan) **in the queue of each approval level**. To see the queue, change "Your Role" to the appropriate level (e.g., Faculty Senate Executive Committee).
- **Programs** https://nextcatalog.marshall.edu/programadmin/
  - Use this link to view **program** proposals. To search, enter an asterisk (*) before keywords or CIM key (e.g., *political science).

Program Additions

College of Arts and Media

New Major: BA, Music Industry
CIM Key (Program): 906

- **Rationale:** This program is replacing the suspended BA in Commercial Music to satisfy accreditation standards set by our accrediting body. This proposal offers a real opportunity for the MU School of Music to take the lead in developing an innovative, sustainable, forward-looking degree opportunity for students who do want to pursue or do not fit in the traditional conservatory model. Additionally, it will be paired with a newly created MU record label and publishing company. A second emphasis area in sound production is forthcoming. Marshall will be an innovative leader in preparing students for new paradigms in the music industry.

New Area of Emphasis: Music Management
CIM Key (Program): 910

- **Major within which it will be listed:** BA, Music Industry

- **Rationale:** This program is replacing the suspended BA in Commercial Music to satisfy accreditation standards set by our accrediting body. This proposal offers a real opportunity for the MU School of Music to take the lead in developing an innovative, sustainable, forward-looking degree opportunity for students who do want to pursue or do not fit in the traditional conservatory model. Additionally, it will

University Curriculum Committee
RECOMMENDATION

SR 24-25-25 CC Recommends approval of the listed **UNDERGRADUATE PROGRAM ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

be paired with a newly created MU record label and publishing company. A second emphasis area in sound production is forthcoming. Marshall will be an innovative leader in preparing students for new paradigms in the music industry.

College of Health Professions

New Majors [CIM Program Key in Brackets]: Athletic Training [879]; Biomechanics [880]; Exercise Science [881]; Strength and Conditioning [882]; Kinesiology [883].

- **Rationale:** This is a Major in the new B.S. Health and Movement Sciences (BSHMS). The BSHMS degree program combines 3 existing degree programs moving the current degree programs as majors

New Areas of Emphasis [CIM Program Key in Brackets]: AT, Pre-Physical Therapy [884]; AT, Pre-Med [885]; AT Pre-Physician Assistant [886].

- **Major within which they will be listed:** Athletic Training

- **Rationale:** Moving an existing AofE to allow students to couple professional program preparation directly to their major.

New Areas of Emphasis [CIM Program Key in Brackets]: Biomec Pre-Physical Therapy [887]; Biomec, Pre-Med [888]; Biomec Pre-Physician Assistant [889].

- **Major within which they will be listed:** Biomechanics

- **Rationale:** Moving an existing AofE to allow students to couple professional program preparation directly to their major.

New Areas of Emphasis [CIM Program Key in Brackets]: Ex Sci, Pre-Physical Therapy [890]; Ex Sci Pre-med [891]; Ex Sci Pre-Physician Assistant [892].

- **Major within which they will be listed:** Exercise Science

- **Rationale:** Moving an existing AofE to allow students to couple professional program preparation directly to their major.

University Curriculum Committee
RECOMMENDATION

SR 24-25-25 CC Recommends approval of the listed **UNDERGRADUATE PROGRAM ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:
New Areas of Emphasis [CIM Program Key in Brackets]: SC, Pre-Med [893]; SC, Pre-Physical Therapy [894]; SC, Pre-Physician Assistant [895].

- **Major within which they will be listed:** Strength and Conditioning

- **Rationale:** Moving an existing AofE to allow students to couple professional program preparation directly to their major.

New Areas of Emphasis [CIM Program Key in Brackets]: Kin, Pre-Physical Therapy [896]; Kin, Pre-Med [897]; Kin, Pre-Physician Assistant [898].

- **Major within which they will be listed:** Kinesiology

- **Rationale:** Moving an existing AofE to allow students to couple professional program preparation directly to their major.

New Degree Program: BS Health & Movement Sci Degre (B.S.)
CIM Key (Program): 901

- **Rationale:** The School of Health and Movement Sciences (SHMS), housed within the College of Health Professions, currently offers degree programs in Athletic Training, Biomechanics, and Exercise Science. Each of these programs has a foundational core stemming from the study of kinesiology. The SHMS is proposing to consolidate these programs into a single degree program, the B.S. in Health and Movement Sciences (BSHMS). With our current degree programs common core and new accreditation requirements, we wish to move our current degree programs as majors under a single degree program- B.S. Health and Movement Sciences (BSHMS).

Program Deletion
College of Science
Program to be deleted: Pre-Computer IT (COS) (NON-DEG)
CIM Key (Program): 568

- **Rationale:** This pre-major should have been moved to CECS when CIT moved from COS to CECS or deleted. Per G Michaelson, currently CECS uses pre-CS (pre computer science) for majors in both CIT and CS. Therefore, 568: Pre-Computer IT (COS) can be deleted.

University Curriculum Committee
RECOMMENDATION

SR 24-25-25 CC Recommends approval of the listed **UNDERGRADUATE PROGRAM ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

Program Changes

College of Arts & Media

Change in Major: BFA, Music
CIM Key (Program): 27

- **Change:** Minimum credit hours to 120
- **Rationale**
    - Addition of MUSA 276 Sophomore Hearing (0 credits). The sophomore hearing has been a long-standing requirement in applied music study. As we pivot from paper records, this course gives the School of Music a formal mechanism for tracking this requirement through DegreeWorks.
    - Addition of language regarding the successful completion of MUS 179D Piano Class as one means of satisfying the piano proficiency requirement.

Changes in Areas of Emphasis [CIM Program Key in Brackets]: Perform, BFA Music Emphasis [28]; Jazz Studies, Emphasis [30]; Multidisciplinary Studies [31].

- **Change:** Minimum credit hours to 120
- **Rationale**
    - Addition of MUSA 276 Sophomore Hearing (0 credits). The sophomore hearing has been a long-standing requirement in applied music study. As we pivot from paper records, this course gives the School of Music a formal mechanism for tracking this requirement through DegreeWorks.
    - Addition of language regarding the successful completion of MUS 179D Piano Class as one means of satisfying the piano proficiency requirement.

University Curriculum Committee
RECOMMENDATION

SR 24-25-25 CC Recommends approval of the listed **UNDERGRADUATE PROGRAM ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:
Change in Minor: Music Entrepreneurship (MINU)
CIM Key (Program): 703

- **Change:** Minimum credit hours to 15

- **Rationale:** The Music Industry major is replacing the suspended BA in Commercial Music to satisfy accreditation standards set by our accrediting body. The music entrepreneurship minor also needed revising to clarify the focus of its curriculum. A separate music/sound production minor will be proposed in the future.

College of Health Professions

Change in Minor: Social Work, Minor (MINU)
CIM Key (Program): 726

- **Changes:**
  - Suspend admissions to the program
  - Change minimum credit hours to 15

- **Rationale:** The social work minor does not provide a comprehensive understanding of the roles and responsibilities of social workers in 21st century practice settings. Those non-majors who take the minor are not receiving the scope of skills and abilities provided by social workers due to the constraints of accreditation that prevent them from taking practice-focused coursework that can only be accessed by majors. This minor will be replaced with 2 undergraduate certificate programs that will enable participants to have a structured set of elective coursework that provides specific baccalaureate content information in healthcare and child welfare social work practice settings.

Division of Aviation

Change in Major: BS, Professional Pilot
CIM Key (Program): 789

- **Changes:**
  - Change degree program code to FL20P
  - Change degree program to BS, Professional Pilot Deg Prg

University Curriculum Committee
RECOMMENDATION

SR 24-25-25 CC Recommends approval of the listed **UNDERGRADUATE PROGRAM ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

- Areas of emphasis exist: Change to No

- Change minimum credit hours to 120

Rationale: Per Nancy Ritter, AVSC 241 needs removed from the curriculum and MGT 348 needs added in its place. AVSC 241 was only taught one time. In the meantime, Degree Works exceptions have been made for currently enrolled students for this course substitution.

FACULTY SENATE CHAIR:

APPROVED BY THE
FACULTY SENATE: _____ DATE: _____

DISAPPROVED BY THE
FACULTY SENATE: _____ DATE: _____

UNIVERSITY PRESIDENT:

APPROVED: _____ DATE: _____

DISAPPROVED: _____ DATE: _____

COMMENTS: _____

_____

_____

_____

University Curriculum Committee
RECOMMENDATION

SR 24-25-26 CC Recommends approval of the listed **UNDERGRADUATE COURSE ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

INSTRUCTIONS: To view each full proposal (including all forms and attachments), log in to Courseleaf CIM using your MU credentials from the links below

- **All Proposals (by Approval Level)** https://nextcatalog.marshall.edu/courseleaf/approve/
  - Use this link to view **all proposals** (courses/programs/miscellaneous/intents-to-plan) **in the queue of each approval level**. To see the queue, change "Your Role" to the appropriate level (e.g., Faculty Senate Executive Committee).
- **Courses** https://nextcatalog.marshall.edu/courseadmin/
  - Use this link to view **course** proposals. To search, enter an asterisk (*) before keywords or CIM key (e.g., *political science).

Course Additions

College of Arts and Media

MUSP 225: Intro to Music Industry
CIM Key (Course): 16026

- **Course Description:** An introduction to the music industry and music production, covering recording, music publishing, live performance, and artist management, while highlighting the roles of artists, songwriters, producers, managers, lawyers, and agents.
- **Credit Hours:** 3
- **CIP Code:** 500901 - Music, General
- **Rationale:** This course will be an integral part of the BA in Music Industry (formerly, BA, Commercial Music) and the Music Entrepreneurship and is designed to introduce students to the music business discipline and the skills and tools they will develop.

MUSP 475: Music Industry Capstone
CIM Key (Course): 16029

- **Course Description:** Students will synthesize concepts of music industry study to create a capstone project.
- **Credit Hours:** 3
- **Prerequisite:** MUSP 495 with a minimum grade of C
- **CIP Code:** 500901 - Music, General

SR 24-25-26 CC Recommends approval of the listed **UNDERGRADUATE COURSE ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

- **Rationale:** This course will help students integrate the skills, knowledge, and experiences amassed through study of the music industry to create a tangible representation of their qualifications.

College of Health Professions

DTS 315: Sports & Performance Nutrition
CIM Key (Course): 16022

- **Course Description:** Develops skills for implementing evidenced based strategies to fuel athletes for the purpose of promoting optimal performance and recovery.
- **Credit Hours:** 3
- **CIP Code:** 513101 - Dietetics/Dietitian
- **Rationale:** Sports and performance nutrition is a rapidly growing area of practice, and Marshall has no undergraduate courses that specifically address the topic. The course will be a welcome addition for Nutrition and Dietetics, Athletic Training, Health Sciences, and Biomechanics majors, to name a few. It will be an elective course option in the newly proposed Nutrition minor. It is anticipated that the course will be offered annually and expected enrollment is 30 students.

College of Science

CHM 425: Brownie, Beer, Bacon Chemistry
CIM Key (Course): 16031

- **Course Description:** The application of biochemistry and physical chemistry to foods and fermented beverages. Kitchen activities and tastings are employed to demonstrate chemical principles.
- **Credit Hours:** 3
- **Prerequisites:** CHM 356 or CHM 327; or consent of instructor
- **Rationale:** This course offers students a unique opportunity to apply concepts learned in general, organic, biological, and physical chemistry to food and fermented beverages. Throughout the course, emphasis is placed on how science can be interpreted for the general public. The course is the only one in the chemistry curriculum that exposes students to the fields of food science and brewing chemistry and therefore is an important opportunity to introduce other possible career paths for chemistry majors. The course also meets the practical needs of students pursuing degrees in chemistry. Majors in Chemistry are required to take chemistry elective

SR 24-25-26 CC Recommends approval of the listed **UNDERGRADUATE COURSE ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

courses to fulfill their degree requirements and some students complain that there is a lack of courses to choose from. There is also a need for additional graduate courses in chemistry that can be cross-listed with undergraduate courses so that they may be delivered within the teaching workload of the faculty. There is high demand for this course as evidenced by enrollments (close to the kitchen capacity of 20 students) when it was offered twice previously as a special topics course. This proposed course will likely be offered every other year with a projected enrollment of 20 students.

PS 101L: Introductory Astronomy Lab
CIM Key (Course): 15941

- **Course Description:** Laboratory to accompany PS 101, focuses on the Solar System, stars and their lifecycles, the Milky Way, the origin and evolution of the Universe, the search for life elsewhere, and related topics.
- **Credit Hours:** 1
- **Corequisite:** PS 101 Introductory Astronomy
- **Rationale:** We are updating our Introductory Astronomy courses to better accommodate our students by splitting the lecture and lab sections. This change will allow us to increase enrollment in the lecture section and offer more flexibility with multiple lab sections, accommodating the high demand and diverse needs of our students

Course Changes

College of Arts and Media

ART 218: Foundations: Site/Matrix
CIM Key (Course): 644

Changes

- Change title to Foundations: Surface/Matrix
- Change course description to “Introduction to fiber art and textile design in one half-semester workshop and printmaking processes in another. Students will develop visual, technical, and critical thinking skills by solving conceptual problems.”

Rationale: This foundations-level course is comprised of two half-semester workshops, one of which is now focusing less on "installation art made with fibers" and more on fiber art and textiles as a whole. This subtle shift away from installation art is the result of teaching more of this in a different foundations-level course (ART 215) and also better

SR 24-25-26 CC Recommends approval of the listed **UNDERGRADUATE COURSE ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

aligns with the objective that half of ART 218 serve as an introductory experience to fiber-based materials and textiles rather than site-specific sculpture. Modifying the course description and changing part of the title from "Site" to "Surface" better reflects the nature of the projects being assigned in this workshop and also more effectively supports the program area of fibers, an established emphasis in the BFA in Visual Art degree. (These changes do not affect Matrix, the other workshop in this course.)

MUS 101: Basic Musicianship [10480]; MUS 110: The Professional Musician [10484]; MUS 326: Music Industry Law [15447]; MUS 495: Music Internship [10874]
CIM Key (Course) in [Brackets]

Changes

- Change alpha designator to MUSP

Rationale: The School of Music is renumbering its courses using new, more specific alpha designators.

MUS 310: Music Perf Arts Entrepreneurship
CIM Key (Course): 10676

Changes

- Change alpha designator to MUSP
- Change title to Music Entrepreneurship
- Change course number to 325
- Change credit hours to 3

Rationale

- Title: To make it more specific to the music industry.
- Credit Hours: This course is being expanded to three days a week and three hours credit to allow for more in-depth study of entrepreneurship as it applies to the music industry and the functions, techniques and problems of management in music business.

University Curriculum Committee
RECOMMENDATION

SR 24-25-26 CC Recommends approval of the listed **UNDERGRADUATE COURSE ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

MUS 327: Music Business I
CIM Key (Course): 10685

Changes

- Change alpha designator to MUSP
- Change credit hours to 3

Rationale

- Alpha designator: The School of Music has undertaken a renumbering of its courses in anticipation of revisions to curricula.
- Credit hours: Course content has been expanded to cover record labels, recording contracts, and recording royalties. This expansion coincides with the newly created MU record label and publishing company.

MUS 427: Music Business II
CIM Key (Course): 10824

Changes

- Change alpha designator to MUSP
- Change credit hours to 3

Rationale

- Alpha designator: The School of Music has undertaken a renumbering of its courses in anticipation of revisions to curricula.
- Credit hours: Course content has been expanded to cover music publishing, musical groups, and music merchandising.

College of Health Professions

NUR 418: Contemporary Nursing
CIM Key (Course): 11284

Changes

- Change course description to “Focus on foundational knowledge to competently address nursing issues in an ever-evolving healthcare landscape.”

University Curriculum Committee
RECOMMENDATION

SR 24-25-26 CC Recommends approval of the listed **UNDERGRADUATE COURSE ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

- Change outcomes to

	Course Student Learning Outcomes
	The student will explore the impact of various forces on health care delivery that may include economic, legal, political, social, ethical, and technological forces/issues.
	The student will apply knowledge of components of effective leadership and management activities including effective communication, delegation, prioritization, nursing care delivery models, and the budgetary process at the institutional level.
	The student will use an ethical decision-making framework for resolving ethical dilemmas in healthcare.
	The student will analyze recently proposed legislation for its impact on nursing/healthcare in the state or nation. (? Possible covered in number 1)
	The student will analyze workforce issues affecting professional nursing practice including the staffing regulations, the nursing shortage, workforce advocacy, conflict resolution, and collective bargaining and unionization.
	Students will be able to improve professional writing skills and strategies through the utilization of various types of formal and informal writings.

Rationale: The faculty does not wish to change the course, just the course description and the course objectives. These better meet the needs and what is currently being taught in the course.

University Curriculum Committee
RECOMMENDATION

SR 24-25-26 CC Recommends approval of the listed **UNDERGRADUATE COURSE ADDITION, DELETION, CHANGE** in the following college and/or schools/programs:

College of Science

PS 101 : Introductory Astronomy (CT)
CIM Key (Course): 12463

Changes

- Change credit hours to 3
- Add corequisite of PS 101L

Rationale: We are updating our Introductory Astronomy courses to better accommodate our students by splitting the lecture and lab sections.
This change will allow us to increase enrollment in the lecture section and offer more flexibility with multiple lab sections, accommodating the high demand and diverse needs of our students.

FACULTY SENATE CHAIR:

APPROVED BY THE
FACULTY SENATE: _____ DATE: _____

DISAPPROVED BY THE
FACULTY SENATE: _____ DATE: _____

UNIVERSITY PRESIDENT:

APPROVED: _____ DATE: _____

DISAPPROVED: _____ DATE: _____

COMMENTS: _____

ACADEMIC PLANNING COMMITTEE
RECOMMENDATION

SR 24-25-27 APC

Recommends the approval of the intent to plan a Bachelor of Science in Sonography at Marshall University.

INSTRUCTIONS: To view each full proposal (including all forms and attachments), log in to Courseleaf CIM using your MU credentials from the links below

- **All Proposals (by Approval Level)** https://nextcatalog.marshall.edu/courseleaf/approve/
  - Use this link to view **all proposals** (courses/programs/miscellaneous/intents-to-plan) **in the queue of each approval level**. To see the queue, change "Your Role" to the appropriate level (e.g., Faculty Senate Executive Committee).
- **Intents-to-Plan** https://nextcatalog.marshall.edu/intentadmin/
  - Use this link to view **intent-to-plan** proposals. To search, enter an asterisk (*) before keywords or CIM key (e.g., *political science).

RATIONALE:
CIM Key: 9

The School of Medical Imaging, in the Marshall University/St. Mary's Center for Education, is seeking to transition the BS in Medical Imaging's sonography area of emphasis into a stand-alone degree program, the Bachelor of Science in Sonography.

Currently sonography is only an area of emphasis within the School of Medical Imaging. This decreases the number of both sonography and radiology technologist graduates. Providing a sonography major as its own program will increase both the certified sonography and the certified radiology technologist graduates from this institution.

In addition, this existing arrangement of the degree program is complicated by the fact that the current program's first area of emphasis (radiography) is accredited by the Joint Review Committee on Education in Radiologic Technology (JRCERT), and the second (sonography) is accredited by the Commission on Accreditation of Allied Health Education Programs (CAAHEP). While JRCERT is recognized by the United States Department of Education, the CAAHEP is not.

To streamline these offerings, Marshall's College of Health Professions and St. Mary's Center for Education, are submitting this Intent to Plan to transition the BS in Medical Imaging's area of emphasis into a stand-alone degree program, the Bachelor of Science in Sonography.

ACADEMIC PLANNING COMMITTEE
RECOMMENDATION

SR 24-25-27 APC

Recommends the approval of the intent to plan a Bachelor of Science in Sonography at Marshall University.

The cost to the university would be minimal if any as this would be a contractual agreement in which the Center for Education would pay administrative fees to the university for services rendered in execution of the curriculum. There is a high demand for certified sonographers within health care, making this program of paramount importance to health care in the region and to our students.

The intention is to have the program ready to implement for the Fall 2025 semester with the understanding that it may need to be moved to Fall 2026. All contractual programs must be approved by the Higher Education Learning Commission (HLC) prior to launch.

FACULTY SENATE CHAIR:

APPROVED BY THE
FACULTY SENATE: _____ DATE: _____

DISAPPROVED BY THE
FACULTY SENATE: _____ DATE: _____

UNIVERSITY PRESIDENT:

APPROVED: _____ DATE: _____

DISAPPROVED: _____ DATE: _____

COMMENTS: _____

_____

_____

Executive Committee
RECOMMENDATION

SR 24-25-28 EC Recommends Amending UPGA-10 Information Security Policy

In accordance with Administrative Procedure 20 (Admin 20), the Executive Committee recommends amending UPGA 10 Information Security Policy as distributed.

Rationale:

FACULTY SENATE CHAIR:

APPROVED BY THE

FACULTY SENATE: _____ DATE:_____

DISAPPROVED BY THE

FACULTY SENATE: _____ DATE:_____

UNIVERSITY PRESIDENT:

APPROVED: _____ DATE:_____

DISAPPROVED: _____ DATE:_____

COMMENTS:

_____

_____

_____

_____

_____

_____

UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

Policy No. UPGA-10

INFORMATION SECURITY POLICY

1.1. General Information:

- Statutory References: WV. Code § 18 B-1-6
- Passage Date: September 12, 2019
- Effective Date: October 15, 2019

1.2. Scope:

This Policy applies to all faculty, staff and third-party Agents of the University as well as any other University affiliates who are authorized to access Institutional Data.

1.3. Background:

Marshall University (University") has adopted the following Information Security Policy ("Policy") as a measure to protect the confidentiality, integrity and availability of institutional Data as well as any Information Systems that store, process or transmit Institutional Data

2. Definitions:

2.1. "Agent" For the purpose of this Policy, is defined as any third-party that has been contracted by the University to provide a set of services and who stores, processes or transmits Institutional Data as part of those services.

2.2. University Information Technology Council ("ITC") The official university committee advising university wide policy for Information Technology Resources usage at Marshall University. The council will create subcommittees as needed, with membership beyond itself to facilitate its work.

2.3. "Information System" is defined as any electronic system that stores, processes, or transmits information.

2.4. "Institutional Data" is defined as any data that is owned or licensed by the University

3. Policy:

3.1. Throughout its lifecycle, all Institutional Data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved by the CIO and maintained by the Information Security Officer, given the level of sensitivity, value and criticality that the Institutional Data has to the University.

3.2. Any Technology Resources that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate according to the ITG-4 Guideline for Data Classification.

3.3. Individuals who are authorized to access Institutional Data shall adhere to the administrative procedure ITP-27 Information Security Roles and Responsibilities, as defined in documentation approved by the CIO and maintained by the Information Security Officer.

3.4. Maintenance:

This Policy will be reviewed by the University's Information Security Office on an annual basis or as deemed appropriate based on changes in technology or regulatory requirements.

3.5. Enforcement:

Violations of this Policy may result in suspension or loss of the violator's use of or privileges to Institutional Data and University owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal, and equitable remedies may apply.

3.6. Exceptions:

Exceptions to this Policy must be approved by the Information Security Office, under the guidance of the Chief Information Officer and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

4. Related Policies, Administrative procedures and Guidelines

4.1. Information Security Roles and Responsibilities
http://www.marshall.edu/itc/itcpolicies&procedures/pdf/itp-27.pdf

4.2. Guidelines for Data Classification
http://www.marshall.edu/itc/itcpolicies&procedures/pdf/itg-4.pdf

4.3. Marshall University IT Information Security Incident Response Procedure
http://www.marshall.edu/itc/itcpolicies&procedures/pdf/itp-19.pdf

UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

Policy No. UPGA-10

INFORMATION SECURITY POLICY

1 General Information:

- Statutory References: WV. Code § 18 B-1-6
- Passage Date: September 12, 2019
- Effective Date: October 15, 2019
- Updated Date: February 20, 2025

1.2. Scope:

This Policy applies to all faculty, ~~staff~~staff, and third-party Agents of Marshall~~the~~ University as well as any other University ~~affiliate~~agents who are authorized to access Institutional Data.

1.3. Background:

Marshall University ("University") has adopted the following Information Security Policy ("Policy") as a measure to protect the confidentiality, ~~integrity~~integrity, and availability of Institutional Data as well as any Information Systems that store, ~~process~~process, or transmit Institutional Data.

2 Definitions:

2.1. "Agent" For the purpose of this Policy, is defined as any third-party that has been contracted by the University to provide a set of services and ~~who~~ stores, ~~processes or~~processes or transmits Institutional Data as part of those services.

~~**2.2.** University Information Technology Council ("ITC") The official university committee advising university wide policy for Information Technology Resources usage at Marshall University. The council will create subcommittees as needed, with membership beyond itself to facilitate its work.~~

~~**2.3.**~~**2.2.** "Information System" is defined as any electronic system that stores, processes, or transmits information.

2.3. "Institutional Data" is defined as any data that is owned or licensed by the University, or its agent.

Formatted: Font: 12 pt

Formatted ...

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted ...

Formatted ...

~~2.4.~~

~~1~~3 **Policy:**

~~1.1~~3.1. Throughout its lifecycle, all Institutional Data shall be protected in a manner that is ~~consistent with the Guideline for~~ Data Classification ~~considered reasonable and appropriate, as defined in documentation approved by the CIO and maintained by the Information Security Officer~~, given the level of sensitivity, value and criticality that the Institutional Data has to the University and its agents. ~~Any Technology Resources~~ that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate according to the ~~ITG-4~~ Guideline for Data Classification.

~~1.2~~3.2. Individuals who are authorized to access Institutional Data shall adhere to the ~~administrative procedure ITP-27~~ Information Security Roles and Responsibilities, as defined in ~~documentation approved by the CIO and maintained by the Information Security Officer.~~this document.

~~1.3 Maintenance:~~

3.3. This Policy will be reviewed by the University's Information Security Office on an annual basis or as deemed appropriate based on changes in technology or regulatory requirements.

3.4. Some violations of this Policy may occur unknowingly and will be addressed in collaboration with MUIT and the employee. However, serious or repeated violations of this Policy may result in restricted or revoked access to Institutional Data and University-owned Information Systems. In cases of extreme or willful misconduct, further administrative actions may be taken, up to and including termination of employment or contractor status, in accordance with existing policies and procedures. In certain situations, civil or legal consequences may also apply.

~~1.4 Enforcement:~~

~~Violations of this Policy may result in suspension or loss of the violator's use of or privileges to Institutional Data and University-owned Information~~

Violations of this Policy may result in further investigation. Wi~~Systems. Additional~~ ~~administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal, and equitable remedies may apply.~~

~~1.5 Exceptions:~~

~~Exceptions to this Policy must be approved by the Information Security Office, under the guidance of the Chief Information Officer and formally~~

3.5. Exceptions to this Policy must be approved by the Information Security Office, under the guidance of the Chief Information Officer and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Formatted: Font: 12 pt, Not Bold, Condensed by 0.1 pt
Formatted: Normal, No bullets or numbering
Formatted: Font: 12 pt, Bold, Not Expanded by / Condensed by
Formatted: List Paragraph, Space Before: 0 pt, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: 0.38", Left + Not at 0.25"
Formatted: Font: Not Bold, Condensed by 0.1 pt
Formatted: Font: 12 pt, Condensed by 0.1 pt, Highlight
Formatted …
Formatted …
Formatted …
Formatted: Condensed by 0.1 pt
Formatted …
Formatted …
Formatted …
Formatted …
Formatted …
Formatted: Condensed by 0.1 pt
Formatted …
Formatted: Highlight
Formatted …
Formatted: Highlight
Formatted …
Formatted …
Formatted …
Formatted: Condensed by 0.1 pt
Formatted …
Formatted …

~~2 Related Policies, Administrative procedures and Guidelines~~

~~2.1 Information Security Roles and Responsibilities http://www.marshall.edu/itc/itcpolicies&procedures/pdf/itp-27.pdf~~

~~2.2 Guidelines for Data Classification http://www.marshall.edu/itc/itcpolicies&procedures/pdf/itg-4.pdf~~

~~Marshall University IT Information Security Incident Response Procedure http://www.marshall.edu/itc/itcpolicies&procedures/pdf/itp-19.pdf~~

4 Information Security Roles and Responsibilities

4.1. Chief Information Officer

The Chief Information Officer (CIO) is a senior-level executive responsible for the overall technology strategy and implementation at the University. Responsibilities of the CIO include the following:

- Developing and implementing the University's IT strategy to support the institution's goals and objectives.
- Overseeing the management of IT infrastructure, including hardware, software, networks, and data centers.
- Ensuring the reliability, security, and scalability of the University's IT systems.
- Evaluating and implementing new technologies to improve efficiency and effectiveness.
- Ensuring compliance with relevant regulations and standards related to IT and data management.
- Developing and maintaining relationships with external vendors and partners.

4.2. Chief Information Security Officer

The Chief Information Security Officer (CISO) is a senior-level employee of the University who oversees the University's information security program. Responsibilities of the CISO include the following:

- Developing and implementing a university-wide information security program.
- Documenting and disseminating information security policies and procedures.
- Coordinating the development and implementation of a university-wide information security training and awareness program.
- Coordinating a response to actual or suspected breaches in the confidentiality, integrity, or availability of Institutional Data.

Commented [JP1]: Current procedure is not considered a university policy. Will be incorporated into this document: Information Security Roles and Responsibilities (marshall.edu)

Formatted: Heading 2, Right: 0", Space Before: 0 pt, Line spacing: single, No bullets or numbering, Tab stops: Not at 0.38" + 0.63"

Commented [JP2]: Current procedure is not considered a university policy. Will be incorporated into this document:

Commented [JP3]: Current procedure is not considered a university policy. Will be incorporated into this document:

Formatted: Font: Bold, No underline, Underline color: Auto, Font color: Auto, Not Expanded by / Condensed by

Formatted: Font: 12 pt

Formatted: Font: Not Bold

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted: Font: Not Bold

Formatted: Bulleted + Level: 1 + Aligned at: 0.59" + Indent at: 0.84"

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted ...

Formatted ...

Formatted: Font: 12 pt

4.3. Chief Data Officer

The Chief Data Officer (CDO) is a senior-level executive responsible for the governance and utilization of data as a strategic asset at the University. Responsibilities of the CDO include the following:

- Developing and implementing a data governance framework to ensure the quality, integrity, and security of Institutional Data.
- Overseeing data management practices and ensuring that data is used effectively across the University.
- Establishing data policies and standards to guide data collection, storage, processing, and usage.
- Ensuring compliance with data-related regulations and standards, including privacy laws and data protection regulations.
- Leading the data management team and coordinating with Data Stewards and Data Custodians.
- Identifying opportunities for data integration and analytics to enhance the University's operations and services.

4.4. Data Steward

A Data Steward is a senior-level employee of the University who oversees the lifecycle of one or more sets of Institutional Data. Responsibilities of the Data Steward include the following:

- Assign appropriate classification to Institutional Data by its sensitivity, value, and criticality of the University as defined by the Guidelines for Data Classification.
- Assign day-to-day administrative and operational responsibilities for Institutional Data to Data Custodians.
- Approve standards and procedures related to the day-to-day operational management of Institutional Data.
- Determine the appropriate criteria for obtaining access to Institutional Data. Provisioning access is the responsibility of the Data Custodian, or the assigned Data Steward based on the business function or support role.
- Ensure that Data Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of Institutional Data.

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted: Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

Formatted: Normal, Indent: Left: 0.34"

Formatted: Font: Not Bold

Formatted: Bulleted + Level: 1 + Aligned at: 0.59" + Indent at: 0.84"

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: 12 pt

Formatted: Font: Not Bold

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted: Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

- Understand and approve how Institutional Data is stored, processed, and transmitted by the University and/or third-party agents of the University.
- Define risk tolerances and accept or reject related security threats that impact the confidentiality, integrity, and availability of Institutional Data.
- Understand legal obligations and cost of non-compliance of data protections.
- Understand how Institutional Data is governed by university policies, State and Federal Regulations, Contracts, and other binding agreements.

4.5. Data Custodian

A Data Custodian is an employee of the University who has ~~dministrative~~administrative and/or operational responsibility to oversee Institutional Data. In many cases, there will be multiple Data Custodians. Data Custodian responsibilities are responsible for the following:

- Understand and report on how Institutional Data is stored, processed, and transmitted by the University, its agents, and third-party agenda of the University.
- Implement appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of Institutional Data.
- Document and disseminate administrative and operational procedures to ensure consistent storage, retention, processing, and transmission of Institutional Data.
- Provision and deprovision access to Institutional Data as authorized by the Data Steward.
- Understand and report security risks and how they impact the confidentiality, integrity, and availability of Institutional Data.

4.6. Users

Users are any employee, contractor, agent, or third-party agent of the University who has authorized access to University Systems and/or Institutional Data. A user is responsible for the following:

- Adhere to policies, guidelines, and procedures pertaining to the protection of Institutional Data.
- Report suspected vulnerabilities in the confidentiality, integrity, or availability of Institutional Data to the Information Security office.

Formatted: Font: 12 pt

Formatted: Bulleted + Level: 1 + Aligned at: 0.59" + Indent at: 0.84"

Formatted: Font: Not Bold

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted: Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

Formatted: Bulleted + Level: 1 + Aligned at: 0.59" + Indent at: 0.84"

Formatted: Font: Not Bold

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted: Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

5 Information Security Awareness & Training

Any user with an account at Marshall University must complete the following annual information security trainings. Failure to complete these trainings may include disruption to your university account and/or te rmination of your university account.

- General Information Security Awareness Training (mandatory for all), including Phishing Awareness and FERPA training.
- GLBA Training (mandatory for any working with student financial accounts)
- HIPAA Training (mandatory for any working with Personal Health Information)
- PCI Training (mandatory for any working with payment card transactions)

6 Guidelines for Data Classification

Employees, agents, and third-party agents of Marshall University should be mindful and only utilize approved acceptable tools and services when storing, processing, and/or transmitting Institutional Data. Technology tools and services, even those at no cost to the University, must be reviewed according to ITP-3: Technology Governance and Procurement Review. This includes personal productivity technologies, including artificial intelligence (AI) tools, that process and retain data (i.e., meeting recording and transcription, large language models (LLMs), small language models (SLMs), image processors, etc.) If there are technology tools or services not listed in the Data Classification Guide, the CIO and the CISO should be notified via e-mail to vet through and information review and be approved accordingly. The Data Classification Guide will be reviewed and updated semi-annually by MUIT.

Table 6.1: Data Classification Guide

Type of Data	Description of Data	Examples of Data	Exposure Risk	Acceptable Tools & Services
Restricted	Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could	- Data protected by state or federal privacy regulations. (i.e., FERPA, HIPAA) - Data protected by confidentiality agreements. - Accounts Payable Information	High	- Blackboard LMS - Banner Student - Banner Finance - Banner HR

Formatted: Font: 12 pt

Formatted: List Paragraph, Indent: Left: 0.84"

Formatted: Right: 0", Space Before: 0 pt, Line spacing: single, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

Formatted: Font: 12 pt, Underline

Formatted: Indent: Left: 0.88", No bullets or numbering

Formatted: Font: 12 pt

Formatted: Right: 0", Space Before: 0 pt, Line spacing: single, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

Formatted: Font: 12 pt, Bold

Formatted: Right: 1.3", Space Before: 6.05 pt, Line spacing: Multiple 1.08 li, Tab stops: 0.38", Left + 0.63", Left

Formatted: Centered

	cause a significant level of risk to the University or its agents.	- Bank Account Information - Employee Personnel Information - Student Loan/Financial Aid Information - Student Advising Information - Student Conduct Information - Enrollment Data - Student Health Data (i.e., Immunizations) - Donor Information - Building Utilities & Life Safety Information - Legal documents and litigation-related information - Network security information. - Critical infrastructure control systems information		- Banner Document Management - Dynamic Forms - OneDrive - Oracle Cloud Infrastructure (OCI) and associated data tables - MS Teams Files - SharePoint - E-Mail (only if ENCRYPT feature is used) - Qualtrics - Salesforce CRM - EAB Navigate - Exxat (Dietetics and Physical Therapy only) - Titanium (Speech and Hearing only) - Symplicity Advocate - StarRez (for the Landing only) - eResLife - Synchronizing files from OneDrive/MS Teams/Sharepoint to a Device is NOT ALLOWED for restricted data, unless device is encrypted. - PHI only allowable for M365, Titanium, and Exxat Software. - TouchNet Student Account Center, Advisor, e-Refunds
Private	Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its agents.	- By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. - University Budget Detail Information - Chart of Accounts & Ledger Information - Procurement Information & Contracts - Research Proposals & Grants	Medium	- All the above - E-Mail does NOT have to be encrypted for this data. - Synchronizing files between One Drive/MS Teams/SharePoint is

Formatted: List Paragraph, Space Before: 12 pt, After: 12 pt, Don't add space between paragraphs of the same style, Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.25"

		- Limited Directory Information - Building Egress Plans - Room Utilization Data - Non-disclosure agreements (NDAs) and other contractual documents - Internal audit reports - Detailed IT infrastructure documents		permitted for Private information. - Adobe Express, Adobe Creative Cloud, Adobe Acrobat Pro DC - Copilot.Microsoft.com -
Public	Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its agents.	- Public Record Information - Press Releases - Course Information - Research Publications - General Directory Information - Campus Map - University policies and procedures that are publicly available. - Event announcements and community outreach information - Award and recognition information for faculty, staff, and students	Low	- No restrictions on storing or sending this type of data.

6.1. Guidelines for Storing, Processing, & Transmitting Restricted Information

As noted, restricted information is any data that when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its agents. The following provides best practices and guidelines for storing, processing, or transmitting restricted information:

- SharePoint sites must indicate visual cues of restricted information storage, access must be limited to only those with a need to know.
- Do not include restricted information in the subject line of a meeting or appointment on your calendar. Ensure the meeting details are protected via access controls or marked “Private.”
- Do not download restricted information to a computing or mobile device unless device encryption is in place. Personally owned equipment and software should NEVER be used to process, store, or transmit restricted information.
- Do not share passwords. If you need to share or remember passwords, utilize a password management software approved by the Information Security Office.
- Do not leave paper copies of restricted information unattended. Ensure restricted information is

Formatted: List Paragraph, Space Before: 12 pt, After: 12 pt, Don't add space between paragraphs of the same style, Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.25"

Formatted: List Paragraph, Space Before: 12 pt, After: 12 pt, Don't add space between paragraphs of the same style, Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.25"

Formatted: Font: 12 pt

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted: Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Font: 12 pt

secured and shredded when no longer needed.

- Do not e-mail restricted information. Instead send a copy of the information via a secure, access-controlled link. Alternatively, utilize the "ENCRYPT" feature in e-mail to encrypt the transmission of the message.
- Do not use personal e-mail to conduct business or e-mail restricted information to a personal account.
- All systems storing restricted information must be reviewed and approved by the Information Security Office. Any systems storing, processing, or transmitted restricted information must utilize Multi-Factor Authentication standards (MFA).
- Keep in mind that FERPA and PHI is considered restricted information. Any data beyond "directory" level information should be considered restricted information. Note: MUID numbers, also known as "901" numbers are considered restricted information. For more information, visit FERPA – Consumer Information and Disclosures (marshall.edu).
- All university printers must be reviewed and approved by Marshall University Information Technology.

7 Technical Controls & Guidelines

7.1. VPN Access

VPN access provides users access to the University network and systems from a remote location. When connected to the university network (onsite or through VPN), information may be collected to ensure security and compliance. This information includes authentication attempts, device configuration compliance, unusual traffic patterns, duration of connection, latency, throughput, bandwidth utilization, and any anomalies.

VPN access will be audited, reviewed, and approved annually. VPN access is granted through the IT Service Desk, upon approval by an employee's direct supervisor and must meet the following requirements:

Multi-Factor Authentication (MFA) must be enabled

- the user's device is encrypted
- the user's device is registered for routine security updates, and has anti-malware software installed

Formatted: Bulleted + Level: 1 + Aligned at: 0.59" + Indent at: 0.84"
Formatted: Font: 12 pt
Formatted: Font: 12 pt, Bold
Formatted: Normal, No bullets or numbering
Formatted: Font: 12 pt, Bold
Formatted: Font: 12 pt, Bold
Formatted: Indent: Left: 0.38", Right: 0", Space Before: 0 pt, Line spacing: single, No bullets or numbering, Tab stops: Not at 0.63"
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Font: 12 pt
Formatted: Normal, Indent: Left: 0.38", No bullets or numbering
Formatted: Font: 12 pt
Formatted: Font: 12 pt

- the user's device is a university managed device

To ensure optimal security when accessing the university network through VPN, the VPN connection will timeout after thirty (30) minutes of inactivity. Additionally, the maximum connection time of the VPN will be twelve (12) hours before reauthentication is required.

7.2. Device Administrative Access

In general, most users do not require administrative access to their university managed device. Device administrative access is granted through the IT Service Desk, upon approval by an employee's direct supervisor. Device administrative access is audited, reviewed, and approved annually.

7.3. Device Encryption

MUIT requires device encryption for any devices that have the potential to store restricted information, including FERPA and HIPAA data. Additionally, external file storage such as hard drives or USB drives must be approved by MUIT Information Security and encrypted when handling restricted information.

7.4. System Logging & Auditing

MUIT routinely collects logs on activities utilizing the University network. System logs will be retained for up to one year to ensure MUIT can conduct compliance reviews and investigations. MUIT also regularly monitors and analyzes log data to detect suspicious activities and identify potential security risks. Only authorized personnel in MUIT will have access to log data. Log data includes the following:

- Startup and shutdown events
- System errors and/or updates
- User activities including login attempts, file access, and changes to user permissions
- Network traffic information including source and destination IP Addresses, port numbers, and protocols
- Application logs including error messages, transaction records, and user activity
- Alerts and logs from security tools such as firewalls, intrusion detection systems, and endpoint detection software

7.5. Guest Accounts

Guest Accounts are provided to non-employees of Marshall University. Guest accounts require a university sponsor and will be audited, reviewed, and approved annually.

Formatted: Font: 12 pt

Formatted: Indent: Left: 0.38", No bullets or numbering

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted: Bulleted + Level: 1 + Aligned at: 0.63" + Indent at: 0.88"

Formatted: Condensed by 0.1 pt

Formatted: Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

Formatted: Font: 12 pt

Formatted: Font: 12 pt, Condensed by 0.1 pt

- Access to enterprise systems and Institutional Data must be approved by the employee's supervisor or guest account sponsor, as well as the Data Steward (or designee). Access to enterprise systems and Institutional Data will be audited, reviewed, and approved annually by the Data Steward (or designee) and the employee's supervisor or guest account sponsor.
- The University will participate in annual penetration testing to ensure the security of its information technology infrastructure and network. Any remediations will be coordinated by the Information Security Office and may include the participation and cooperation of other units and/or employees of the University.
- Marshall University Information Technology may collect and audit system transaction log files to detect and respond to security incidents in a timely manner. This may include user access, administrative actions, system errors, and security events.

7.6. Security Audits & Risk Assessments

MUIT participates in a variety of security audits and assessments. MUIT will routinely test and monitor the effectiveness of our technical safeguards through these assessments.

8 Vendor Risk Management

All technology systems or services used by the University, its agents, or third-party agents must undergo an information security review, as outlined in ITP-3: Technology Governance and Procurement Review. The Information Security Office utilizes the Higher Education Community Vendor Assessment Toolkit (HECVAT) provided by Educause to assess risk for technology vendors. The HECVAT is a questionnaire framework specifically designed for higher education to measure vendor risk. Elevated risk technologies or those that do not meet the standards herein must be approved by the Technology Executive Council, as well as the Chief Legal Counsel of the University.

9 Information Security Incident Response Procedure

9.1. Incident Definition:

An incident is the act of violating an explicit or implied security policy. These include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data resulting in an unwanted disruption or denial of service.

Formatted: Not Expanded by / Condensed by

Formatted: Normal, Indent: Left: 0.38", Right: 0", Space Before: 8 pt, Line spacing: single, Tab stops: Not at 0.63"

Formatted: Font: 12 pt

Formatted: Font: Not Bold

Formatted: Normal, No bullets or numbering

Formatted: Font: 12 pt

Formatted: Right: 0", Space Before: 0 pt, Line spacing: single, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

Formatted: Font: 12 pt

Formatted: Right: 0", Space Before: 0 pt, Line spacing: single, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

Formatted: Font: 12 pt, Condensed by 0.1 pt

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

- the unauthorized use of a system for the processing or storage of data,
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

All MU employees, agents, and third-party agents are required to report any activities that meet these incident criteria. It is our policy to keep any information specific to the incident confidential.

9.2. Incident Response Procedure:

- Step 1 - Information Security office and the IT Response Team is notified that a potential or actual breach has occurred through one of the following modalities: 1) IT Service Desk, 2) Direct Contact (i.e., Incident Response Form or e-mail abuse@marshall.edu), 3) Legal Counsel, Campus Police, or other Law Enforcement Agencies, 4) Internal/External Audit groups, 5) Human Resources, 6) External or Internal Complaints/Observations, etc.
- Step 2 – Determination of Severity

  Determination of the level of severity are as follows:

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: 12 pt

Formatted: Indent: Left: 0.08", Hanging: 0.3", Right: 0", Space Before: 8 pt, Line spacing: single, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.08" + Indent at: 0.38", Tab stops: Not at 0.63"

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: List Paragraph, Indent: Left: 0.84"

Severity	Symptoms
1	• Network or system outage with significant impact to the user population or operation of the University. • High probability of propagation. • Probable or actual release or compromise of sensitive data (financial records, personal data, passwords, etc.) • Requires immediate remedial action to prevent further compromise of data and adverse impact to network or other entities. • Notification of entities outside the University is required.
2	• Some adverse impact to the operation of the University. • Adverse effects are localized or contained, or minimal risk of propagation. • No apparent release or compromise of sensitive data. • Remedial but not immediate action is required. • Notification of entities within the University is required.

3	• Minimal impact to small segment of user population or operation of university. • Completely localized, with few individuals affected, and presenting little or no risk to other entities. • No loss or compromise of sensitive data. • Remedial action is required. • Individual notification is required.

- Step 4 – Initial Notification of Incident: Based on the determined severity level, the following will receive an initial notification of the incident. All Severity 1 incidents require the formation of an Incident Response Team.
    - Severity 1: President, Chief of Staff, Chief Legal Counsel, Chief Information Officer, Chief Data Officer, Provost, Chief Financial Officer, Chief Marketing & Communications Officer, Chief of Police, others as determined.
    - Severity 2: Chief Legal Counsel, Chief Information Officer, Chief Data Officer, others as determined.
    - Severity 3: Chief Legal Counsel, Chief Information Officer, Chief Data Officer, others as determined. Notifications for this severity level will be sent post investigation.
- Step 5 – Investigation: The IT Information Security designate meets with the reporting organization or personnel to discuss and begin the investigation and documentation of the incident. The investigation proceeds as rapidly as possible to a highly probable conclusion of Severity Level. A preliminary report and Severity Level determination is provided to the Information Security within 48 hours. Investigation will include the following questions:
    - What happened?
    - What systems, devices, etc., were compromised?

Formatted ...
Formatted: Left, Right: 0.27", Line spacing: Exactly 12.6 pt
Formatted: Right: 0.27", Line spacing: Exactly 12.6 pt
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted: Indent: Left: 0.84", No bullets or numbering
Formatted
Formatted ...
Formatted: Font: 12 pt
Formatted ...
Formatted: Bulleted + Level: 2 + Aligned at: 1.09" + Indent at: 1.34"
Formatted ...

- What is the net damage and costs?
- Was information lost or stolen? If yes, what?
- Was the information restricted or private?
- How was the information acquired?
- How was the system or device configured?
- What are the maintenance procedures?
- Do log files exist?
- Who was affected by the breach?

- Step 6: Determine level of external involvement needed included the following:
  - WV-BRIM
  - Law Enforcement
  - Cyber-Security consulting services
  - Others, as identified.
- Step 7: Documentation & Remediation will include the following processes:
  - Preservation of evidence
  - Determine root cause.
  - Implement required technology remediations.
  - File criminal charges (if required)
- Step 8: Develop & Implement Communication Plan for all notifications and media outreach.
  - Notification letters should contain the following: 1) a description of the breach, 2) Contact information for major credit reporting agencies, 3) recommendation to place a fraud alert on respective credit reports and ongoing monitoring, 4) a university contact for additional information.

Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted: Font: 12 pt
Formatted: Bulleted + Level: 2 + Aligned at: 1.09" + Indent at: 1.34", Tab stops: 0.73", Left + Not at 0.81"
Formatted
Formatted ...

- Notifications of security incidents will be sent via first class mail on university letterhead to impacted individuals.
- University Marketing and Communications will follow established policies and procedures for media relations and notifications.
- All media inquiries or questions should be directed to the Chief Information Officer, Chief Information Security Officer, or a member of University Marketing & Communications.

~~2.3~~• Step 9: Conclusion & Final Report; The Information Security Office will provide a final report to all identified stakeholders.

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Right: 0", Space Before: 9.1 pt, Line spacing: single, Bulleted + Level: 1 + Aligned at: 0.59" + Indent at: 0.84", Tab stops: 0.73", Left + Not at 0.38" + 0.63"

Formatted: Font: Not Bold

UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

Policy No. UPGA-10
INFORMATION SECURITY POLICY

1 General Information:

- Statutory References: WV. Code § 18 B-1-6
- Passage Date: September 12, 2019
- Effective Date: October 15, 2019
- Updated Date: February 20, 2025

1.2. Scope:

This Policy applies to all faculty, staff, and third-party Agents of Marshall University as well as any other University agents who are authorized to access Institutional Data.

1.3. Background:

Marshall University ("University") has adopted the following Information Security Policy ("Policy") as a measure to protect the confidentiality, integrity, and availability of Institutional Data as well as any Information Systems that store, process, or transmit Institutional Data.

2 Definitions:

2.1. "Agent" For the purpose of this Policy, is defined as any third-party that has been contracted by the University to provide a set of services and stores, processes or transmits Institutional Data as part of those services.

2.2. "Information System" is defined as any electronic system that stores, processes, or transmits information.

2.3. "Institutional Data" is defined as any data that is owned or licensed by the University, or its agent.

3 **Policy:**

3.1. Throughout its lifecycle, all Institutional Data shall be protected in a manner that isconsistent with the Guideline for Data

Classification , given the level of sensitivity, value and criticality that the Institutional Data has to the University and its agents.Any Technology Resource that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate according to the Guideline for Data Classification.

3.2. Individuals who are authorized to access Institutional Data shall adhere to the Information Security Roles and Responsibilities, as defined in this document.

3.3. This Policy will be reviewed by the University's Information Security Office on an annual basis or as deemed appropriate based on changes in technology or regulatory requirements.

3.4. Some violations of this Policy may occur unknowingly and will be addressed in collaboration with MUIT and the employee. However, serious or repeated violations of this Policy may result in restricted or revoked access to Institutional Data and University-owned Information Systems. In cases of extreme or willful misconduct, further administrative actions may be taken, up to and including termination of employment or contractor status, in accordance with existing policies and procedures. In certain situations, civil or legal consequences may also apply.

3.5. Violations of this Policy may result in further investigation. Wil Exceptions to this Policy must be approved by the Information Security Office, under the guidance of the Chief Information Officer and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

4 Information Security Roles and Responsibilities

4.1. Chief Information Officer

The Chief Information Officer (CIO) is a senior-level executive responsible for the overall technology strategy and implementation at the University. Responsibilities of the CIO include the following:

- Developing and implementing the University's IT strategy to support the institution's goals and objectives.
- Overseeing the management of IT infrastructure, including hardware, software, networks, and data centers.
- Ensuring the reliability, security, and scalability of the University's IT systems.
- Evaluating and implementing new technologies to improve efficiency and effectiveness.
- Ensuring compliance with relevant regulations and standards related to IT and data management.

- Developing and maintaining relationships with external vendors and partners.

4.2. Chief Information Security Officer

The Chief Information Security Officer (CISO) is a senior-level employee of the University who oversees the University's information security program. Responsibilities of the CISO include the following:

- Developing and implementing a university-wide information security program.
- Documenting and disseminating information security policies and procedures.
- Coordinating the development and implementation of a university-wide information security training and awareness program.
- Coordinating a response to actual or suspected breaches in the confidentiality, integrity, or availability of Institutional Data.

4.3. Chief Data Officer

The Chief Data Officer (CDO) is a senior-level executive responsible for the governance and utilization of data as a strategic asset at the University. Responsibilities of the CDO include the following:

- Developing and implementing a data governance framework to ensure the quality, integrity, and security of Institutional Data.
- Overseeing data management practices and ensuring that data is used effectively across the University.
- Establishing data policies and standards to guide data collection, storage, processing, and usage.
- Ensuring compliance with data-related regulations and standards, including privacy laws and data protection regulations.
- Leading the data management team and coordinating with Data Stewards and Data Custodians.
- Identifying opportunities for data integration and analytics to enhance the University's operations and services.

4.4. Data Steward

A Data Steward is a senior-level employee of the University who oversees the lifecycle of one or more sets of Institutional Data. Responsibilities of the Data Steward include the following:

- Assign appropriate classification to Institutional Data by its sensitivity, value, and criticality of the University as defined by the Guidelines for Data Classification.
- Assign day-to-day administrative and operational responsibilities for Institutional Data to Data Custodians.
- Approve standards and procedures related to the day-to-day operational management of Institutional Data.
- Determine the appropriate criteria for obtaining access to Institutional Data. Provisioning access is the responsibility of the Data Custodian, or the assigned Data Steward based on the business function or support role.
- Ensure that Data Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of Institutional Data.
- Understand and approve how Institutional Data is stored, processed, and transmitted by the University and/or third-party agents of the University.
- Define risk tolerances and accept or reject related security threats that impact the confidentiality, integrity, and availability of Institutional Data.
- Understand legal obligations and cost of non-compliance of data protections.
- Understand how Institutional Data is governed by university policies, State and Federal Regulations, Contracts, and other binding agreements.

4.5. Data Custodian

A Data Custodian is an employee of the University who has administrative and/or operational responsibility to oversee Institutional Data. In many cases, there will be multiple Data Custodians. Data Custodian responsibilities are responsible for the following:

- Understand and report on how Institutional Data is stored, processed, and transmitted by the University, its agents, and third-party agenda of the University.
- Implement appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of Institutional Data.
- Document and disseminate administrative and operational procedures to ensure consistent storage,

retention, processing, and transmission of Institutional Data.

- Provision and deprovision access to Institutional Data as authorized by the Data Steward.
- Understand and report security risks and how they impact the confidentiality, integrity, and availability of Institutional Data.

4.6. Users

Users are any employee, contractor, agent, or third-party agent of the University who has authorized access to University Systems and/or Institutional Data. A user is responsible for the following:

- Adhere to policies, guidelines, and procedures pertaining to the protection of Institutional Data.
- Report suspected vulnerabilities in the confidentiality, integrity, or availability of Institutional Data to the Information Security office.

5 Information Security Awareness & Training

Any user with an account at Marshall University must complete the following annual information security trainings. Failure to complete these trainings may include disruption to your university account and/or te

rmination of your university account.

- General Information Security Awareness Training (mandatory for all), including Phishing Awareness and FERPA training.
- GLBA Training (mandatory for any working with student financial accounts)
- HIPAA Training (mandatory for any working with Personal Health Information)
- PCI Training (mandatory for any working with payment card transactions)

6 Guidelines for Data Classification

Employees, agents, and third-party agents of Marshall University should be mindful and only utilize approved acceptable tools and services when storing, processing, and/or transmitting Institutional Data. Technology tools and services, even those at no cost to the University, must be reviewed according to ITP-3: Technology Governance and Procurement Review. This includes personal productivity technologies, including artificial intelligence (AI) tools, that process and retain data (i.e., meeting recording and transcription, large language

models (LLMs), small language models (SLMs), image processors, etc.) If there are technology tools or services not listed in the Data Classification Guide, the CIO and the CISO should be notified via e-mail to vet through and information review and be approved accordingly. The Data Classification Guide will be reviewed and updated semi-annually by MUIT.

Table 6.1: Data Classification Guide

Type of Data	Description of Data	Examples of Data	Exposure Risk	Acceptable Tools & Services
Restricted	Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its agents.	- Data protected by state or federal privacy regulations. (i.e., FERPA, HIPAA) - Data protected by confidentiality agreements. - Accounts Payable Information - Bank Account Information - Employee Personnel Information - Student Loan/Financial Aid Information - Student Advising Information - Student Conduct Information - Enrollment Data - Student Health Data (i.e., Immunizations) - Donor Information - Building Utilities & Life Safety Information - Legal documents and litigation-related information - Network security information. - Critical infrastructure control systems information	High	- Blackboard LMS - Banner Student - Banner Finance - Banner HR - Banner Document Management - Dynamic Forms - OneDrive - Oracle Cloud Infrastructure (OCI) and associated data tables - MS Teams Files - SharePoint - E-Mail (only if ENCRYPT feature is used) - Qualtrics - Salesforce CRM - EAB Navigate - Exxat (Dietetics and Physical Therapy only) - Titanium (Speech and Hearing only) - Symplicity Advocate - StarRez (for the Landing only) - eResLife - Synchronizing files from OneDrive/MS Teams/Sharepoint to a

				Device is NOT ALLOWED for restricted data, unless device is encrypted. - PHI only allowable for M365, Titanium, and Exxat Software. - TouchNet Student Account Center, Advisor, e-Refunds
Private	Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its agents.	- By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. - University Budget Detail Information - Chart of Accounts & Ledger Information - Procurement Information & Contracts - Research Proposals & Grants - Limited Directory Information - Building Egress Plans - Room Utilization Data - Non-disclosure agreements (NDAs) and other contractual documents - Internal audit reports - Detailed IT infrastructure documents	Medium	- All the above - E-Mail does NOT have to be encrypted for this data. - Synchronizing files between One Drive/MS Teams/SharePoint is permitted for Private information. - Adobe Express, Adobe Creative Cloud, Adobe Acrobat Pro DC - Copilot.Microsoft.com -
Public	Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its agents.	- Public Record Information - Press Releases - Course Information - Research Publications - General Directory Information - Campus Map - University policies and procedures that are publicly available. - Event announcements and community outreach information - Award and recognition information for faculty, staff, and students	Low	- No restrictions on storing or sending this type of data.

6.1. Guidelines for Storing, Processing, & Transmitting Restricted Information

As noted, restricted information is any data that when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its agents. The following provides best

practices and guidelines for storing, processing, or transmitting restricted information:

- SharePoint sites must indicate visual cues of restricted information storage, access must be limited to only those with a need to know.
- Do not include restricted information in the subject line of a meeting or appointment on your calendar. Ensure the meeting details are protected via access controls or marked "Private."
- Do not download restricted information to a computing or mobile device unless device encryption is in place. Personally owned equipment and software should NEVER be used to process, store, or transmit restricted information.
- Do not share passwords. If you need to share or remember passwords, utilize a password management software approved by the Information Security Office.
- Do not leave paper copies of restricted information unattended. Ensure restricted information is secured and shredded when no longer needed.
- Do not e-mail restricted information. Instead send a copy of the information via a secure, access-controlled link. Alternatively, utilize the "ENCRYPT" feature in e-mail to encrypt the transmission of the message.
- Do not use personal e-mail to conduct business or e-mail restricted information to a personal account.
- All systems storing restricted information must be reviewed and approved by the Information Security Office. Any systems storing, processing, or transmitted restricted information must utilize Multi-Factor Authentication standards (MFA).
- Keep in mind that FERPA and PHI is considered restricted information. Any data beyond "directory" level information should be considered restricted information. Note: MUID numbers, also known as "901" numbers are considered restricted information. For more information, visit FERPA – Consumer Information and Disclosures (marshall.edu).
- All university printers must be reviewed and approved by Marshall University Information Technology.

7 Technical Controls & Guidelines

7.1. VPN Access

VPN access provides users access to the University network and systems from a remote location. When connected to the university network (onsite or through VPN), information may be collected to ensure security and compliance. This information includes authentication attempts, device configuration compliance, unusual traffic patterns, duration of connection, latency, throughput, bandwidth utilization, and any anomalies.

VPN access will be audited, reviewed, and approved annually. VPN access is granted through the IT Service Desk, upon approval by an employee's direct supervisor and must meet the following requirements:

Multi-Factor Authentication (MFA) must be enabled

- the user's device is encrypted
- the user's device is registered for routine security updates, and has anti-malware software installed
- the user's device is a university managed device

To ensure optimal security when accessing the university network through VPN, the VPN connection will timeout after thirty (30) minutes of inactivity. Additionally, the maximum connection time of the VPN will be twelve (12) hours before reauthentication is required.

7.2. Device Administrative Access

In general, most users do not require administrative access to their university managed device. Device administrative access is granted through the IT Service Desk, upon approval by an employee's direct supervisor. Device administrative access is audited, reviewed, and approved annually.

7.3. Device Encryption

MUIT requires device encryption for any devices that have the potential to store restricted information, including FERPA and HIPAA data. Additionally, external file storage such as hard drives or USB drives must be approved by MUIT Information Security and encrypted when handling restricted information.

7.4. System Logging & Auditing

MUIT routinely collects logs on activities utilizing the University network. System logs will be retained for up to one year to ensure MUIT can conduct compliance reviews and investigations. MUIT also regularly monitors and analyzes log data to detect suspicious activities and identify potential security risks. Only authorized personnel in MUIT will have access to log data. Log data includes the following:

- Startup and shutdown events
- System errors and/or updates
- User activities including login attempts, file access, and changes to user permissions
- Network traffic information including source and destination IP Addresses, port numbers, and protocols
- Application logs including error messages, transaction records, and user activity
- Alerts and logs from security tools such as firewalls, intrusion detection systems, and endpoint detection software

7.5. Guest Accounts

Guest Accounts are provided to non-employees of Marshall University. Guest accounts require a university sponsor and will be audited, reviewed, and approved annually.

- Access to enterprise systems and Institutional Data must be approved by the employee's supervisor or guest account sponsor, as well as the Data Steward (or designee). Access to enterprise systems and Institutional Data will be audited, reviewed, and approved annually by the Data Steward (or designee) and the employee's supervisor or guest account sponsor.
- The University will participate in annual penetration testing to ensure the security of its information technology infrastructure and network. Any remediations will be coordinated by the Information Security Office and may include the participation and cooperation of other units and/or employees of the University.
- Marshall University Information Technology may collect and audit system transaction log files to detect and respond to security incidents in a timely manner. This may include user access, administrative actions, system errors, and security events.

7.6. Security Audits & Risk Assessments

MUIT participates in a variety of security audits and assessments. MUIT will routinely test and monitor the effectiveness of our technical safeguards through these assessments.

8 Vendor Risk Management

All technology systems or services used by the University, its agents, or third-party agents must undergo an information security review, as outlined in ITP-3: Technology Governance and Procurement Review. The

Information Security Office utilizes the Higher Education Community Vendor Assessment Toolkit (HECVAT) provided by Educause to assess risk for technology vendors. The HECVAT is a questionnaire framework specifically designed for higher education to measure vendor risk. Elevated risk technologies or those that do not meet the standards herein must be approved by the Technology Executive Council, as well as the Chief Legal Counsel of the University.

9 Information Security Incident Response Procedure

9.1. Incident Definition:

An incident is the act of violating an explicit or implied security policy. These include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data resulting in an unwanted disruption or denial of service.
- the unauthorized use of a system for the processing or storage of data,
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

All MU employees, agents, and third-party agents are required to report any activities that meet these incident criteria. It is our policy to keep any information specific to the incident confidential.

9.2. Incident Response Procedure:

- Step 1 - Information Security office and the IT Response Team is notified that a potential or actual breach has occurred through one of the following modalities: 1) IT Service Desk, 2) Direct Contact (i.e., Incident Response Form or e-mail abuse@marshall.edu), 3) Legal Counsel, Campus Police, or other Law Enforcement Agencies, 4) Internal/External Audit groups, 5) Human Resources, 6) External or Internal Complaints/Observations, etc.
- Step 2 – Determination of Severity

  Determination of the level of severity are as follows:

Severity	Symptoms
1	• Network or system outage with significant impact to the user population or operation of the University. • High probability of propagation. • Probable or actual release or compromise of sensitive data (financial records, personal data, passwords, etc.) • Requires immediate remedial action to prevent further compromise of data and adverse impact to network or other entities. • Notification of entities outside the University is required.
2	• Some adverse impact to the operation of the University. • Adverse effects are localized or contained, or minimal risk of propagation. • No apparent release or compromise of sensitive data. • Remedial but not immediate action is required. • Notification of entities within the University is required.

3	• Minimal impact to small segment of user population or operation of university. • Completely localized, with few individuals affected, and presenting little or no risk to other entities. • No loss or compromise of sensitive data. • Remedial action is required. • Individual notification is required.

- Step 4 – Initial Notification of Incident: Based on the determined severity level, the following will receive an initial notification of the incident. All Severity 1 incidents require the formation of an Incident Response Team.
    - Severity 1: President, Chief of Staff, Chief Legal Counsel, Chief Information Officer, Chief Data Officer, Provost, Chief Financial Officer, Chief Marketing & Communications Officer, Chief of Police, others as determined.
    - Severity 2: Chief Legal Counsel, Chief Information Officer, Chief Data Officer, others as determined.
    - Severity 3: Chief Legal Counsel, Chief Information Officer, Chief Data Officer, others as determined. Notifications for this severity level will be sent post investigation.
- Step 5 – Investigation: The IT Information Security designate meets with the reporting organization or personnel to discuss and begin the investigation and documentation of the incident. The investigation proceeds as rapidly as possible to a highly probable conclusion of Severity Level. A preliminary report and Severity Level determination is provided to the Information Security within 48 hours. Investigation will include the following questions:
    - What happened?
    - What systems, devices, etc., were compromised?

- What is the net damage and costs?
- Was information lost or stolen? If yes, what?
- Was the information restricted or private?
- How was the information acquired?
- How was the system or device configured?
- What are the maintenance procedures?
- Do log files exist?
- Who was affected by the breach?

- Step 6: Determine level of external involvement needed included the following:
  - WV-BRIM
  - Law Enforcement
  - Cyber-Security consulting services
  - Others, as identified.
- Step 7: Documentation & Remediation will include the following processes:
  - Preservation of evidence
  - Determine root cause.
  - Implement required technology remediations.
  - File criminal charges (if required)
- Step 8: Develop & Implement Communication Plan for all notifications and media outreach.
  - Notification letters should contain the following: 1) a description of the breach, 2) Contact information for major credit reporting agencies, 3) recommendation to place a fraud alert on respective credit reports and ongoing monitoring, 4) a university contact for additional information.

- Notifications of security incidents will be sent via first class mail on university letterhead to impacted individuals.
- University Marketing and Communications will follow established policies and procedures for media relations and notifications.
- All media inquiries or questions should be directed to the Chief Information Officer, Chief Information Security Officer, or a member of University Marketing & Communications.

- Step 9: Conclusion & Final Report: The Information Security Office will provide a final report to all identified stakeholders.