University of Wisconsin-Madison
Secretary of the Faculty
133 Bascom Hall

FACULTY SENATE MEETING AGENDA MATERIALS for 2 April 2018

The University Committee encourages senators to discuss the agenda with their departmental faculty prior to meeting.

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

FACULTY SENATE AGENDAS, MINUTES, RECORDINGS, TRANSCRIPTIONS AND FACULTY DOCUMENTS, INCLUDING FACULTY POLICIES AND PROCEDURES, ARE AVAILABLE:
secfac.wisc.edu/governance/faculty-senate/

FACULTY SENATE MEETING
Monday, April 2 2018 - 3:30 p.m.
272 Bascom Hall

AG E N D A

1. Memorial Resolutions for:
   Professor Emeritus Mark Brownfield. (Fac doc 2735)
   Professor Emeritus Truman Graf. (Fac doc 2736)
   Professor Emeritus Philip E. Harris (Fac doc 2742)
   Professor Emeritus William Reddan. (Fac doc 2737)

2. Presentation of the 2018 Hilldale Awards to:
   - Arts and Humanities Division: Professor Leslie Bow, Department of English.
   - Biological Sciences Division: Professor Rick Gourse, Department of Bacteriology.
   - Physical Sciences Division: Professor Mark Kenoyer, Department of Anthropology.
   - Social Sciences Division: Professor Guri Sohi, Department of Computer Sciences.

3. Announcements/Information Items.
   UW-Madison Cybersecurity Risk Management Policy. (Fac doc 2738 and Fac doc 2739)

4. Question Period.

5. Minutes of March 5. (*consent*)

6. Proposed changes to Campus Diversity and Climate Committee (CDCC) *Faculty Policies and Procedures* 6.27. (Fac doc 2728) (*vote*)

7. Proposal to Create the Committee on Disability Access and Inclusion (CDAI). *Faculty Policies and Procedures* 6.31. (Fac doc 2729). (*vote*)

8. Retirement of the Advisory Committee for the Office for Equity and Diversity (OED), the Disabilities Accommodation Advisory Committee (DAAC), and the Committee on Access and Accommodation in Instruction (CAAI). (Fac doc 2740) (*vote*)

9. Proposed updates to *Faculty Policies and Procedures*: 6.01., 6.02., 6.03., 6.04., 6.07., 6.09., 6.10., 6.11., 6.12., and 6.49. (Fac doc 2733) (*vote*)

10. Proposed changes to Faculty Policies and Procedures Chapter 7 based on the report from the Ad Hoc Committee on 7th-year Reviews. (Fac doc 2741). (*first reading*)

Memorial Resolution of the Faculty of the University of Wisconsin-Madison
On the Death of Professor Emeritus Mark Brownfield

Dr. Mark Brownfield, Associate Professor Emeritus in the Department of Comparative Biosciences in the School of Veterinary Medicine at the University of Wisconsin-Madison, died on November 21, 2017 at 69 years of age.

Born on February 6, 1948, Professor Brownfield earned his undergraduate degree (Zoology, 1972) and a master's degree (Anatomy, 1977) from Colorado State University. He developed an interest in neuroendocrinology and hypothalamic function working with Dr. Gerald Kozlowski and received his Ph.D degree (Anatomy, 1979) from Colorado State University. From 1968-1978, he also worked as a medical, surgical, and orthopedics nurse at Loveland Memorial Hospital in Loveland, Colorado. He was a postdoctoral fellow with Dr. William Ganong at the University of California-San Francisco where he studied serotonergic neurons, angiotensin, and other neuropeptide hormones.

In 1982, Professor Brownfield became an Assistant Professor in the Department of Comparative Biosciences within the newly established School of Veterinary Medicine at the University of Wisconsin-Madison. His most important and influential work was in the physiological characterization of serotonergic neurons, as well as the localization and function of serotonin receptors. He was highly successful in the design, generation, and testing of antibodies to specific receptors in the brain, especially serotonin receptors. Several of the antibodies that he designed were sold by commercial companies for use by other scientists. The impact of his contributions to neuroscience is substantial when one considers how many hundreds of scientists have used his antibodies over the past several years. Professor Brownfield also collaborated with many other faculty at the University of Wisconsin-Madison while studying neuroendocrine regulation of body fluids, feeding and metabolism, and cardiovascular function.

As a teacher, Professor Brownfield helped to develop the curriculum for the new veterinary school, particularly in the fields of endocrinology and physiology. He taught Endocrine Physiology to every veterinary student who graduated from the School of Veterinary Medicine from the first class that entered in 1983, through the spring of 2016, his last semester before his retirement. He was particularly devoted to providing research opportunities for undergraduate students at the University of Wisconsin-Madison. During a typical semester, Professor Brownfield often had 2-3 undergraduate students working in his laboratory. Accordingly, in 2016, Professor Brownfield was nominated for the university's Award for Mentoring Undergraduate Research Students. Professor Brownfield provided a warm approachable environment in the laboratory that allowed students to freely and openly discuss their career goals. In many cases, Dr. Brownfield's discussion and advice proved to be instrumental in advancing the students' academic careers. Many of his undergraduate students presented posters locally on campus, as well as at national science meetings, and several students have won awards for their presentations. After his retirement and at the time of his passing, he had continued to direct his research laboratory and advise undergraduate researchers.

Professor Brownfield was beloved by his many associates and colleagues. He will be remembered for his caring spirit, sense of humor, and unassuming manner. He was helpful, thoughtful, supportive, and friendly to his colleagues and students. He had limitless generosity in sharing the secrets of successful immunocytochemistry and endless patience while training

(continued)

undergraduates in his lab. He always had time to listen and to talk about science, whether it was neuroendocrinology or astronomy.

Professor Brownfield is survived by his son Andrew Brownfield, daughter Marialisa Brownfield, and their mother, Jane Mahoney, as well as his brothers, Ned and Joseph Brownfield.

Memorial Resolution Committee

Stephen M. Johnson, Associate Professor,
Department of Comparative Biosciences

Linda A Schuler, Professor
Department of Comparative Biosciences

Thaddeus G. Golos, Professor and Chair
Department of Comparative Biosciences

Memorial Resolution of the Faculty of the University of Wisconsin-Madison
On the Death of Professor Emeritus Truman F. Graf

Professor Emeritus Truman Frederick Graf died on Monday, August 7, 2017 at the age of 94. Truman was born and raised on a small, progressive dairy farm near New Holstein, Wisconsin. In the 1920s, long before the Rural Electrification Administration (REA) began to string power lines to Wisconsin farms, Truman's father installed a gas-powered generator to produce electricity to operate milking machines.

With the financial help of merit-based scholarships earned while attending New Holstein High School, Truman enrolled in the University of Wisconsin-Madison after graduation. His undergraduate studies were interrupted when Truman enlisted in the Navy Air Corps shortly after the U.S entered World War II. He was commissioned as a Navy Ensign and trained to pilot a Helldiver Dive Bomber. He continued flying as a Navy Reserve pilot for a few years after the war ended before transferring into Naval Intelligence He continued serving as a Navy Reserve officer throughout his professional career, retiring as a Full Commander after 30 years of service. After his discharge from active military service, Truman returned to UW-Madison to continue his studies, earning a BS degree in Agriculture (1947) and MS and Ph.D. degrees in Agricultural Economics (1949 and 1953). Upon receiving his doctorate, he was hired by the Department of Agricultural Economics as an assistant professor and subsequently promoted to associate professor (1956) professor (1961).

Professor Graf joined the faculty at a time when the Madison campus of the University of Wisconsin was growing rapidly in student and faculty numbers. It was also growing in its commitment to the Wisconsin Idea that the boundaries of the campus coincide with the boundaries of the state. In accord with that commitment, Truman's appointment was largely funded by Cooperative Extension, His responsibilities were to assist farmers, dairy plant managers, cooperative and farm organization leaders, state and federal political leaders and others in promoting their understanding of issues related to milk pricing and marketing and to help them take actions beneficial to Wisconsin's expanding dairy sector.
Truman's dairy farm background, work ethic, engaging personality, and ability to quickly and accurately evaluate and explain complex dairy issues made him a perfect fit for the position. He spoke the language of his clientele. They understood him, trusted him, and benefitted from his well-grounded advice and counsel. He quickly became one of the most sought-after dairy spokesperson, analyst, and advisor in the United States, making countless presentations to constituent groups and frequently providing testimony at administrative and legislative hearings. He was an exemplary Extension specialist and his work enhanced the visibility and stature of the Department and the University.

Truman's work covered the gamut of dairy pricing, marketing and policy issues. He placed particular emphasis on evaluating proposed changes in milk marketing orders and federal dairy policy, equitable pricing of milk, international dairy trade, and dairy promotion. He complemented his Extension program with solid supporting research, often in collaboration with graduate student advisees and colleagues in other states. In addition to his outreach and research, he taught dairy marketing to thousands of undergraduates and Farm and Industry Short Course students.

(continued)

Professor Graf's immense contributions on behalf of dairy interests resulted in several prestigious awards. These included World Dairy Expo Man of the Year, Wisconsin Cooperative Leader Award, National Dairy Shrine Pioneer Award, University of Wisconsin-Extension Distinguished Service Award, and Wisconsin Federation of Cooperatives Cooperative Builder Award. Truman's ability to effectively convey complex economic concepts to lay audiences was recognized by the American Agricultural Economics Association Quality of Communications Award in 1974.

The Department of Agricultural Economics benefitted from Truman's benevolence as well as his academic and service accomplishments. Most notably, in the early 1980s Truman, among others, actively solicited funding to help convert a former dormitory into Taylor Hall, the department's current home. He was personally responsible for generating donations exceeding $100,000, most of that amount coming from dairy cooperatives and state dairy leaders in gratitude for his many years of assistance. A few years later, he spearheaded a funding drive to convert a redundant Taylor Hall bathroom into a graduate student lounge, named in honor of John R. Commons. Donations from dairy cooperatives tallied more than $6,000. In 1989, Truman and his wife, Sylvia, endowed a scholarship to provide financial assistance to undergraduate students majoring in Agricultural Economics and Agricultural Business Management.

Upon his retirement in 1985, Professor Graf began a lengthy "second career" involving dairy development projects overseas. Funded by an array of granting agencies, he provided technical assistance to government authorities in Armenia, Bulgaria, Cuba, Czech Republic, Finland, Honduras, Hungary, Kazakhstan, Poland, Russia, Uganda, Ukraine and Zimbabwe.

Truman's obituary contained his personal view of citizen responsibility, which seems appropriate to this memorial resolution: "My goal in life has been to make a contribution to society which will long outlast my stay on earth. I have attempted to do this through teaching, research, and public service work in my professional field, agricultural economics, and also as a "good citizen" in non-professional related volunteer work. My philosophy of life is that we all owe society far more than it owes us, and I hope to make at least a partial payment on my share of the debt." Truman is survived by Sylvia, his wife of 70 years; their children, Eric, Siri (Bill) and Peter (Barb); grandchildren, Sara and Christopher; and great-grandchildren, Maren and Viggo Masters.

Memorial Resolution Committee

Ed Jesse
Bruce Jones
Kyle Stiegert

Memorial Resolution of the Faculty of the University of Wisconsin-Madison
On the Death of Professor Emeritus Philip E. Harris

Professor Philip E. Harris was a faculty member in the College of Agricultural and Life Science's Department of Agricultural and Applied Economics and University of Wisconsin Extension from 1979 until his retirement in 2016. Over this 37 years Phil taught agricultural law to undergraduates, tax practitioners, farm operators and those living in rural areas.

During his career, Prof. Harris directly touched the lives of thousands, and indirectly, millions of individuals. A lasting legacy of Prof. Harris is his establishment of the Land Grant University Tax Education Foundation and his editorship of 15 annual National Income Tax Workbooks. This text continues to the resource by more than 29,000 professional income tax preparers across 26 states serving of clients across the country. He was also a founding member of the American Agricultural Law Association (AALA) serving as President from 1987-1988. In 1998, Prof. Harris received the AALA Distinguished Service Award for his dedication to making the complexities of agricultural taxation more understandable to both tax practitioners and the agricultural community.

Professor Harris grew up on his family's Iowa farm and graduated from Iowa State University earning a bachelor's degree in Economics. He received both his Masters in Economics and his law degree from the University of Chicago. The combining of his understanding of economics and tax law made Phil truly unique among his peers.

He passed away on January 12, 2018.

Phil was an avid runner. Regardless of the weather, we would always see Phil leaving some time during the day to undertake his daily run. The greatest joy in his life was his family. He is survived by his wife, Karen; son, Seth (Kate) Harris; and daughter, Rachel (Steve) Finch, five grandchildren and three siblings.

The following is just a sampling of the many comments received by his family upon hearing of his terminal illness and then his passing. These comments provide strong evidence of his intellectually abilities, contribution to the agricultural community and commitment to the Wisconsin Idea.

University Faculty Member: ….I just wanted to let you know that my heart is heavy at the passing of Phil. He was always a generous mentor to me, and I regarded him as one of the titans in our field of work. Our agreed sentiment was that we lost one of the greats, and his passing will leave a giant hole in our field of work. Far more importantly, though, we also agreed that we lost a great person…

University Law Professor: Please thank Phil for always being such a wonderful colleague, a model of professionalism, and someone always willing to help. The example that he always provided and the thoughtful, insightful and objective information that he shared with others made such an impact on everyone who had the pleasure of learning from him - whether at conferences, in classrooms, or in a one-to-one. I am so grateful to be an agricultural law colleague and friend.

University of Wisconsin Colleague: Phil, as you go down this road, remember that you will be in our hearts and minds as long as we live. You have been a treasured colleague who I loved to see walk through my office door to chat. You have been the CALS Extension specialist who has been the most frequently called upon for help and who has provided that help most frequently and most comprehensively. You have been largely responsible for ensuring that American farmers are

(continued)

provided the best possible income tax advice. You are a true gentleman and a good friend who will never be forgotten.

Wisconsin County Extension Agent: I just wanted to say how much I appreciate how Phil always made time for Extension Agents and farmers across the state. Phil's impact on Wisconsin agriculture is well known. Phil always responded to questions, and was always willing to meet with farmers out in the counties. Phil helped so many people, and they are greatul. I literally could see on faces how much better they felt after receiving information from Phil that provided clarity to very complicated situations.

Wisconsin County Extension Agent: I was so sorry to hear of Phil's health. It was a true pleasure to work with Phil. I'll always remember how kind he was when I was brand new to the job and still trying to figure things out. He always ha[d] this cool and calm demeanor, even in tough situations. I don't know if it will ever be possible to add up all the farm families Phil has helped. It's a true legacy. I know it took time away from family, but we were so appreciative that Phil was one of the few willing to travel "North of Madison."

Wisconsin County Extension Agent: For more than three decades, Phil has been one of the best UW-Extension specialist I've had the privilege of working with. His expertise in agricultural/tax law was second to none and his teaching/counselling skills are truly the best I've ever seen. From the smallest of rural town halls, to banquet halls in back of a country taverns, to major conference centers across the state, Phil's commitment and support of WI agriculture and county Extension agents will never be forgotten.

Wisconsin Tax Practitioner: I have been in his Eau Claire Tax Insight class for 20 years. …Please tell Phil that he was instrumental in the growth of my tax business! I grew the business from a handful of tax returns done at the kitchen table between farm chores. We milked cows on the family farm of 40 head of Registered Guernsey's. My business now has 2 office locations and this year are on track to process 2000 returns. Yes, 2000!! Not bad for a farm girl that needed a side gig to challenge her mind between milkings. I always looked forward to Phil's classes. He has an amazing gift of being able to convey the complexities of the tax code into verbiage that was so easy to understand. He is such a kind caring individual that faced even the most annoying tax preparers' questions with great poise, professionalism and completeness.… Please let him know how much he has impacted my life!! I am proud to say that because of my tax business, I have had the privilege of being able to help many others far beyond the preparation of the tax return. Much of which is because of the gifts he shared with us at the annual tax classes!!

Wisconsin Dairy Farmer: I wish to say thank you for teaching a just off the dairy farm - wet behind the ears college student all about farm law. I only got a B+ but that was a huge achievement seeing that I had zero knowledge prior to your class. And I enjoyed every day of the class. I cherish every discussion that we had over the last almost 40 years.

In summary, Professor Harris was a generous contributor of service to the Department of Agricultural and Applied Economics, the University of Wisconsin-Madison, University of Wisconsin Extension, the agricultural law profession and society as a whole.

Memorial Resolution of the Faculty of the University of Wisconsin-Madison
On the Death of Professor Emeritus William G. Reddan

Bill Reddan died on December 18, 2017 at age 90. He spent his life serving his family, his country, the greater Madison community, and UW-Madison with extraordinary distinction. Bill was born and raised in St. Louis in a sports and education centered family. He served in the US military in both WWII and Korean Wars, graduated from UW-Madison with an MS, and PhD—the latter achieved in 1965 as the inaugural graduate student in Dr. John Rankin's laboratory of Pulmonary Medicine—and served as a faculty member from 1968 to his retirement in 1996.

Bill was the "founding father" of soccer in Madison and at the UW—serving as founder of the pioneering Madison 56ers club, the Madison Area Youth Soccer Association, and then as the first coach of the UW soccer program, culminating with an NCAA Championship in 1995 under the tutelage of Bill and his protégé, head coach Jim Launder. Bill not only coached the Badgers, he and his late wife Betty made and maintained the uniforms, constructed the goal posts, and provided a loving extended family for the players. His election in to all of our state's soccer and sports halls of fame always prompted the same humble response from Bill: "Geez guys, what's the big deal?!"

Professor Reddan taught anatomy and physiology and researched the physiology of exercise, temperature regulation, and respiratory system aging. Several of Bill's seminal research findings--especially those concerning the physiologic effects of temperature changes during exercise, the effects of lifelong endurance training on the aging lung, and the respiratory adaptations to sustained hypoxic exposure--continue to be relevant and cited today.

Importantly Bill also served as an advisor to the majority of the 68 pre- and postdoctoral trainees in the Rankin Laboratory many of whom have become academic and scientific leaders. Several of them fondly recalled their interactions with Bill. For example,

> "He always had a twinkle in his eye and a genuine love of helping others."
> "I am a better person and the world a better place for having Bill in it."
> "I have especially fond memories of how kind he was to me when I arrived in Madison as a very nervous and lonely postdoc."
> "He taught me more than physiology—lessons that continue to guide me and inspire me to this day."
> "Bill was a mentor of smile and good will to those he touched."

Bill is survived by his children, Howie, Mary, and John, and 3 grandchildren.

Bill Reddan was a good man and a dependable and loyal friend who lived a good and full life in the service and betterment of many of us. Good on ya, Modic!

Memorial Resolution Committee
Jerome A. Dempsey
Edward H. Vidruk

The University of Wisconsin-Madison Cybersecurity Risk Management Policy
as approved by the Information Technology Committee on March 16, 2018

POLICY

Cybersecurity risk will be managed to ensure that the likelihood and impact of threats and vulnerabilities are minimized to the extent practical. Guided by the Principles below, the focus of this policy is the protection of University data and the associated information systems.

The process described in the Implementation Plan of this policy, is the mandatory process for managing the cybersecurity risk associated with all information systems of any kind that store or process data used to accomplish University research, teaching and learning, or administration. Data not owned by the University may fall within the scope of this policy if the data is stored or processed using University assets.

The initial process and any future revisions of the process will be reviewed and approved by IT Governance[1]. Any IT governance group or the Office of Cybersecurity may initiate a revision by contacting the Policy Analysis Team who will engage IT Governance.

The process will be phased in. Restricted Data systems will be first, with Sensitive and Internal then Public systems to follow. The activity level to secure a system will be proportional to the data driven categorization of the information system and intended level of risk with the system in operation.

1. Rates for assessing risk or providing a central hosting service which meets many of the risk management requirements will be developed by the service provider, vetted within IT governance, with final determination by senior campus leadership.
2. Determining funding for risk management activity and compliance matters is the responsibility of each school, college, or division through use of approved sources.

Research, teaching and learning, or administrative systems that have a short life span (less than one year) and present a low risk, or that temporarily present a moderate risk, may be granted a temporary exception by registering and describing the system through the Risk Management Framework package intake process, or its successor or designee. Each system will be evaluated on a case-by-case basis to determine the system risk category, the estimated duration of the risk, and if granted, the duration of the exception.

The Office of Cybersecurity will provide mandatory cybersecurity training for leaders, managers, system developers and users. Training will be appropriate to the audience, and will be phased in over time.

[1] IT Governance is defined at https://it.wisc.edu/it-community/governance/

PRINCIPLES

The University of Wisconsin-Madison is a leading public institution of learning and higher education. As such, our mission is to create and disseminate knowledge and to learn the truth wherever it may be found. Fundamental to this mission is the academic freedom, the "fearless sifting and winnowing" process emblazoned at the entrance to Bascom Hall by the class of 1910.

Recognizing that monitoring and analysis employed for network defense against cybersecurity threats can have a significant chilling effect on learning and academic freedom, the Office of Cybersecurity will operate under the following principles:

1. We respect academic freedom and personal privacy as we help protect the integrity and reputation of the University, and provide a secure and safe computing environment for teaching, research, and outreach.
2. We understand the value of University information as a product of research, teaching, and learning, including the personal data of our faculty, staff, and students.
3. We are committed to ensuring the appropriate security of all data, specifically ensuring that faculty, staff, and student data is not placed at undue risk of exposure.
4. We are accountable to the University community for our deployment and use of network analysis and monitoring tools. Our activity preserves and strengthens the privacy and academic freedom of faculty, staff, students, and other members of our community.
5. We ensure that risk analysis tools and active filtering methods are used only for the detection of malicious activity, and are not used for examining any other content in the data stream.
6. We evaluate the content of system and network traffic only to the extent necessary to detect known security threats or emerging indications of compromised systems. Specifically:
    a. Our tools and techniques are not used to monitor individual activity. Data generated or collected that may identify individual behavior will be retained no longer than is necessary to identify and evaluate malicious traffic.
    b. Data generated is used only to detect threats, vulnerabilities, and compromises. Any personal or private content captured during the testing and detection process is ignored, and is either not recorded at all, or is eliminated immediately in cases where temporary recording is technologically necessary.
    c. Data collected is accessible only by staff responsible for maintaining the security of computing systems, and only for the purpose of diagnosing and remediating security incidents. This data will not be released for any other purpose, except to comply with legal requests.
7. We make decisions on network and cybersecurity defensive measures through a defined and shared process that implements the principles above. We will ensure that our process allows for temporary situations where immediate defensive action is needed, and reviews those temporary measures to determine if they should become ongoing.
8. We implement prevailing cybersecurity practices that reduce or eliminate the potential for impacting Availability, Integrity or Confidentiality of data and information systems.
9. The procedures that implement the Risk Management Framework are developed with collaboration in mind and will be revised collaboratively as conditions warrant.

BACKGROUND

Cybersecurity is a collective responsibility which requires policy that applies to all components of the University of Wisconsin-Madison. Threat, vulnerability and likelihood of exploitation are complex and unique to specific business processes and technologies. Cybersecurity risk is

(continued)

measurable depending on quantified or classified aspects of the data; characteristics of the information system; the definitions and characteristics of internal or external threat, system or environmental vulnerabilities; and the likelihood that the event or situation may manifest itself within a given application, information system or architecture. External threats evolve rapidly and are persistent based on the criminal intent or the resources of the attacker, whether they are criminal or nation state backed. Internal threats can be accidental or intentional.

The impact of using diverse but competing approaches in implementing security controls applied to information systems tends to elevate overall cybersecurity risk[2]. The management of cybersecurity risk will use a detailed Risk Management Framework to balance among academic / business needs, the potential impact of adverse events, and the cost to reduce the likelihood and severity of those events.

1. The risk management process is established in policy so that the University community can share a common understanding that:
2. The University is determined to manage cybersecurity risk effectively. Not doing so is likely to have unacceptable consequences to individuals and increase cost to the institution.
3. This is the University's mandatory and universally applicable process for managing cybersecurity risk. The process can be tailored to specific technologies, processes, or services.
4. The process must include policy and procedural controls to ensure that privacy and academic freedom are respected.

AUTHORITY

This policy was approved by the Information Technology Committee on January 19, 2018 and forwarded to the University Committee. It was presented to the Faculty Senate on February 5, 2018 for information, and issued by the Vice Provost for Information Technology on February 9, 2018.

ENFORCEMENT

Failure to build and maintain information systems that adhere to the policy and principles or which significantly deviate from the Implementation Plan will likely increase risk to University data and information systems. Significant architecture, development or operating and process deviations which result is elevated risk or which impact compliance may result in the following:

1. Computing services or devices may be denied access to University information resources.
2. University employees may be subject to disciplinary action up to and including termination of employment.
3. Contractors or associates may be subject to penalty under the governing agreement. Compliance may be a consideration affecting new or renewed agreements.Contact

Please address questions or comments to the Office of Cybersecurity at cybersecurity@cio.wisc.edu.

[2] From *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute for Standards and Technology, February 2014

Implementation Plan for the University of Wisconsin-Madison Cybersecurity Risk Management Policy

as approved by the Information Technology Committee on March 16, 2018.

This working document is the implementation plan for the Cybersecurity Risk Management Policy. The plan will be reviewed by the community, Information Technology (IT) governance, and the IT Committee.

IMPLEMENTATION

For each information system, the Office of Cybersecurity will maintain a separate and detailed implementation plan that is jointly developed with the System Owner, also known as a System Security Plan. The Office of Cybersecurity will assist distributed Information Technology groups with developing implementation plans tailored to their group's needs.

Data Classifications [1]

The University has classified its institutional data assets into risk based categories for determining who is allowed to access institutional data and what security precautions must be taken to protect it against unauthorized access and use.

Restricted	Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause a significant level of risk to the University, affiliates or research projects. Data should be classified as Restricted if: • protection of the data is required by law or regulation or • The University is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed or disclosed
Sensitive	Data should be classified as Sensitive when the unauthorized disclosure, alteration, loss or destruction of that data could cause a moderate level of risk to the University, affiliates or research projects. Data should be classified as Sensitive if the loss of confidentiality, integrity or availability of the data could have a serious adverse effect on university operations, assets or individuals.
Internal	Data should be classified as Internal when the unauthorized disclosure, alteration, loss or destruction of that data could result in risk to the University, affiliates, or research projects. By default, all Institutional Data that is not explicitly classified as Restricted, Sensitive or Public data should be treated as Internal data.
Public	Data should be classified as Public prior to display on web-sites or once published without access restrictions; and when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates.

[1] From https://data.wisc.edu/data-governance/data-classifications/

(continued)

Risk Levels

Risk is attributed to assets based on the analysis of multiple factors which influence the Availability, Integrity or Confidentiality (AIC) of the asset.

Factors include:

- threats posed to that asset
- the vulnerabilities that expose the asset
- the impact to any of the UW-Madison mission, values or guiding principles and
- the likelihood that the availability, integrity or confidentiality of the asset will be compromised through a given vulnerability by a threat actor.

In a quasi-equation format:

[Risk (to AIC of an asset), (from a threat-vulnerability pairing)] = [the Likelihood of exploitation in a given time frame] X [the impact of such exploitation]

Incidents are categorized based on the severity of potential or actual impact to the university. The graphic below shows the color code as used in the Weekly IT Security Report provided to the University CIO and interested University leadership. Color codes are supported by a short narrative statement that summarizes the major impact of the incident.

Risk Rating Color Code

RISK LEVEL	DESCRIPTION
CRITICAL	Event in progress or significant loss of data and damage to university networks
HIGH	Realized impact to the university
MODERATE	Potential significant impact to the university
LOW	No significant events
NONE	No evidence of risk

Please consult the Office of Cybersecurity if a more detailed discussion is needed or for assistance in the development of a tailored impact score matrix, as well as the building of a Risk Register (not shown) from the resulting scoring.

Risk Registration

Information systems proposed to undergo Risk Assessment are entered into the Risk Register managed by the Office of Cybersecurity. A Risk Analyst will be assigned as resources become available. Organizations desiring to accelerate the process can contact the Chief Information Security Officer for guidance and options for meeting Risk Analyst resource requirements.

Timeline

With the volume of systems and networks at the University, a full implementation of the Risk Management Framework will take approximately five years to complete. Implementation will initially focus on systems handling or storing data classified as Restricted, then Sensitive. Since exposure or loss of Internal or Public data does not pose an immediate operational impact or significant financial risk, those information systems will be reviewed as resources allow.

PRIORITY	CATEGORY	TIMEFRAME
1	Systems with Restricted Data (PII/SSN's, Financial Accounts, HIPAA)	2017 through 2018
2	Research systems where grant funding is tied to security requirements	2017 through 2019 and ongoing
3	New or significantly updated systems with Sensitive Data	2019 - 2020
4	Remaining systems with Sensitive Data	2020 - 2021 and ongoing
5	Systems that only handle Internal Data	2021 - 2022 and ongoing
6	Systems that only handle Public Data	2022 and ongoing

Throughout the implementation period, systems of all kinds will benefit from advanced firewalls and network protections as those capabilities are further deployed. Public facing web servers will be monitored on a monthly basis for unwanted traffic, evidence of cyber-attack or potentially harmful data loss activity to ensure openly accessible data is protected.

Training

Training on the processes, tools and use of or completion of artifacts will be provided by the Office of Cybersecurity with the details considered to be out of scope for this document. Ongoing security awareness training will be provided by the Security Education, Training and Awareness Lead and access to training tools will be widely publicized on the Office of Cybersecurity web pages (https://it.wisc.edu/about/office-of-the-cio/cybersecurity/risk-management-framework/).

Training for Risk Executives will be provided by the Chief Information Security Officer on an individual or group basis depending on the need and executive schedules. Training is tailored to the Risk Executive's needs and will include the items in the Step 5 Accept Risk section, including review of RMF packages aligned with the Risk Executive areas of responsibility.

PROCESS FOR MANAGING CYBERSECURITY RISK

This section describes process specific activities necessary to carry out the Cybersecurity Risk Management Policy. The process steps summarized below are required by the policy. Amplification of process steps and a helpful background on the Risk Management Framework (RMF) are in Appendix A to this Implementation Plan.

Preparation for Risk Assessment

The first three steps of the Risk Management Framework (RMF) prepare the information system for a certifiable risk assessment. As shown in Appendix A, an information system is categorized according to the potential impact should the availability, integrity or confidentially of the system or data be compromised, (RMF Step 1.) Security controls are selected to reduce the likelihood and impact of a compromise, (RMF Step 2.) The security controls are implemented, then tested to measure how well they are functioning, (RMF Step 3.) At this point the information system is ready for a certifiable risk assessment.

Assessing, Accepting and Monitoring Risk

The Cybersecurity Risk Management Policy focuses on the final three steps of the RMF. The following describes the process which is mandated by the policy.

A. Assess Risk (RMF Step 4)

The academic / functional unit and the Office of Cybersecurity cooperatively assess the cybersecurity risk associated with a system and if needed, consultation with other experts on campus.

B. Certify Risk (RMF Step 5)

The University Chief Information Security Officer (CISO) signs the Risk Assessment to certify that the represented risk is accurate. The CISO may include recommended risk reduction strategies.

C. Accept Risk (RMF Step 5)

The risk of operating the system is accepted by the Risk Executive on behalf of The University. This is a leadership decision and should be based on the following:

1. Assessed risk and impact to the University should a system be compromised or data lost.
2. Recommended remediation to include consideration for cost to implement.
3. Impact on the business process should the system, while in operation, lose availability of the system or data, encounter data integrity issues, or breach confidentiality of Restricted or Sensitive data.
4. The Risk Executive role is guided by the following:
   a. Risk Executives will be named within 60 days of the Cybersecurity Risk Management Policy being finalized. The initial list of Risk Executives will be the executives who reported IT spending for their unit as part of the second "IT Spend" report. The units reporting are listed in Appendix B to this implementation plan.
   b. The Risk Executive should be an executive or director, (e.g., Dean or their appointee, department chair, director of a research lab, etc.,) within the academic / functional unit, or in the line of authority above that unit. The Risk Executive must have the authority to accept the risk of operating the system on behalf of the institution and should be in the unit who will ultimately be responsible for paying for a breach (i.e., Dean or their appointee, department, research lab, etc.)
   c. Delegation of the Risk Executive role is not encouraged. If delegation of the work is made under the Risk Executive's authority, the Risk Executive remains accountable for the outcomes.
   d. Risk Executives may access the expertise, training and support available from the Office of Cybersecurity for advice in making their risk determination or for additional guidance.
   e. The Risk Executive must be afforded a sufficient understanding of the information system through the technical experts and managers associated with the system.
   f. The Risk Executive balances the business needs, the potential financial and reputational cost of adverse events, and the cost of reducing the likelihood and severity of those events.
   g. After reviewing the Risk Assessment and recommendations of the Office of Cybersecurity, the Risk Executive will:
      1) accept the risk as certified, or
      2) assure that recommended action is taken to reduce the risk to an acceptable level, or
      3) decline to authorize the system to operate.

h. Training for Risk Executives will be provided by the Chief Information Security Officer on an individual or group basis depending on the need and executive schedules. Training is tailored to the Risk Executive's needs and will include the items in 4.a. through g. above and will include review of a representative RMF package.

D. **Reduce Risk (RMF Step 5 and 6)**

The acceptable level of risk may be constrained by legal, regulatory or contractual requirements, and is subject to review by university leadership.

If the certified level of risk is unacceptable:

1. The Risk Executive assures that changes are made to the system that reduce the risk to an acceptable level.
2. The assessment and certification described in *A. Assess Risk* and *B. Certify Risk* are revised following confirmation of corrective actions. The reduced level of risk is then accepted as described in *C. Accept Risk*.

Following the Risk Assessment and subsequent acceptance by the Risk Executive, information systems with vulnerability, threat and impact changes that elevate the level of risk will have to be corrected or mitigated back to the assessed level (or lower) within the following time limits:

1. Issues that elevate the risk level to Critical should be corrected or mitigated to no greater than High within 72 – 96 hours or the system should be disconnected.
2. Issues that elevate the risk to High should be corrected or mitigated to Moderate within 15 calendar days.
3. Issues that elevate the risk to Moderate should be corrected or mitigated to Low within 90 calendar days.
4. If the issue occurs on a system evaluated at Low risk, but does not elevate the risk to Medium, it should be corrected within one year.

In all cases, the Risk Register maintained by the office of Cybersecurity should be updated along with adjusting the existing risk assessment and plan of action and milestones.

E. **Monitor Risk (RMF Step 6)**

The academic / functional unit and the Office of Cybersecurity continually monitor the system to assure that the level of risk remains at or below the level accepted in *C. Accept Risk*.

1. There must be policy and procedural safeguards to assure that monitoring activity respects privacy and academic freedom.
2. The design and implementation of monitoring is included in the assessment and certification described in *A. Assess Risk* and *B. Certify Risk*. Monitoring must be designed and implemented to, at a minimum:
   a. detect known security vulnerabilities and threats, and
   b. detect known indications that the system may be compromised.
3. Where the identified problems are individually or collectively significant enough to increase the level of risk above the level accepted in *C. Accept Risk*, the identified problems must be sufficiently mitigated, as described in *D. Reduce Risk*, to return the level of risk to the level accepted in *C. Accept Risk*.

F. **Re-evaluate Risk (RMF Step 6)**

Risk evaluation occurs throughout the system life cycle as follows:

1. The schedule for risk evaluation is part of the assessment and certification described in *A. Assess Risk* and *B. Certify Risk*. A typical schedule includes a formal evaluation every three years and an informal evaluation annually.
2. Change management is part of the assessment and certification described in *A. Assess Risk* and *B. Certify Risk*. Changes to the system that increase risk may require more immediate evaluation.
3. Following an evaluation, the assessment and certification described in *A. Assess Risk* and *B. Certify Risk* are revised, the risk is accepted or reduced as described in *C. Accept Risk* and *D. Reduce Risk*, and monitoring continues as described in *E. Monitor Risk*.

Special cases

Non-University-owned devices and services used for university business may be treated as part of a University information system, and if so, are subject to this policy. There must be policy and procedural controls in place to assure respect for property and privacy.

CONTACT

Questions and comments to this document can be directed to the Office of Cybersecurity at cybersecurity@cio.wisc.edu.

REFERENCES

UW-Madison Cybersecurity Risk Management Procedures website [under development], https://it.wisc.edu/about/office-of-the-cio/cybersecurity/risk-management-framework/]

National Institute for Standards and Technology Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

National Institute for Standards and Technology Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems, and Organizations*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute for Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

Controlled Unclassified Information (32 CFR Part 2002), https://www.gpo.gov/fdsys/pkg/FR-2015-05-08/pdf/2015-10260.pdf

BACKGROUND

Risk is defined as the measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence[2].

Cybersecurity risk may be presented from external sources or by individual actions of those working inside the network or information systems. The concept of cybersecurity risk includes operational risk to information and technology assets that have consequences affecting the availability, integrity or confidentiality, of information or information systems. This includes the resulting impact from physical or technical threats and vulnerabilities in networks, computers, programs and data. The data focus includes information flowing from or enabled by connections to digital infrastructure, information systems, or industrial control systems, including but not limited to, information security, supply chain assurance, information assurance, and hardware and software assurance[3].

The process described in this policy is a tool used to arrive at an understanding of risk involving information systems. Risk can be modeled as the likelihood of adverse events over a period of time, multiplied by the potential impact of those events. Risk is never reduced to zero. There is always a level of risk that must be accepted as a cost of doing business. Reducing the risk to an acceptable level is also a cost of doing business. Risk ratings are driven by the Risk Assessment Tool which assigns values to threats, vulnerabilities, and likelihood of exploitation to determine risk.

Systems are monitored to assure that the level of cybersecurity risk is maintained at or below an acceptable level. There are policy and procedural safeguards to assure that personal privacy and academic freedom are respected. The content or use of the data is only of interest to the extent that it indicates the presence of a vulnerability or threat, such as incoming data that is part of an attack on university systems, or outgoing data that indicates a system has already been compromised. University or personal data that is stolen by an attacker is no longer private. Scrupulous monitoring helps protect data from unscrupulous use.

INTERNAL AND EXTERNAL THREAT, VULNERABILITY, AND LIKELIHOOD

Threat, vulnerability and likelihood of exploitation are complex and unique to specific business processes and technology. Cybersecurity risk is measurable depending on quantified or classified aspects of the data; characteristics of the information system; the definitions and characteristics of internal or external threat, system or environmental vulnerabilities; and the likelihood that the event or situation may manifest itself within a given application, information system or architecture. Internal threats can be accidental or intentional. Vulnerabilities are normally discovered outside of the information environment and reported by trusted sources and

---

[2] From NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms*, dated May 2013

[3] From *A Taxonomy of Operational Cyber Security Risks* by James Cebula and Lisa Young, Carnegie-Mellon University Software Engineering Institute, dated December 2010.

characterized against industry norms. The likelihood an event may take place is dependent on the broader spectrum of people, technology and procedures in place to counter the threat and address the vulnerability.

The table below shows broad definitions of cybersecurity issues and the potential risk level that may be assigned to information systems using the Risk Management Framework.

DESCRIPTION	RISK LEVEL
ROOT-LEVEL INTRUSION: an unauthorized person gained root-level access/privileges on a University computer/information system/network device.	**High**
USER-LEVEL INTRUSION: an unauthorized person gained user-level privileges on a University computer/information system/network device.	**High**
ATTEMPTED ACCESS: an unauthorized person specifically targeted a service/vulnerability on a University computer/information system/network device in an attempt to gain unauthorized or increased access/privileges, but was denied access.	**Moderate**
DENIAL OF SERVICE (DOS): use of a University computer/information system/network was denied due to an overwhelming volume of unauthorized network traffic. DOS activity may be reported as High Risk if a significant segment of the University's networks are disabled or if designated Critical Infrastructure / Key Resources are taken off-line.	**Moderate**
POOR SECURITY PRACTICE: a University computer/information system/network was incorrectly configured or a user did not follow established policy. This activity may be rated as Moderate or High if the practice resulted in significant loss of data or denial of service.	**Low**
SCAN/PROBE: open ports on a University computer/information system/network device were scanned with no DOS or mission impact.	**Low**
MALICIOUS CODE (MALWARE): hostile code successfully infected a University computer/information system/network device. Unless otherwise directed, only those computers that were infected will be reported as a Moderate Risk incident unless the malware has disabled a complete information system or significant segment of the University's network.	**Moderate**
SUSPICIOUS ACTIVITY (INVESTIGATION): any identified suspicious activity. The event will be investigated as Low risk, and either dismissed or categorized as one of the above types of activity.	**Low**
EXPLAINED ANOMALY: authorized network activity.	**None**

THE INFORMATION SYSTEM

An information system can be defined as discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control

systems.[4] Each information system should include a security boundary which clearly defines the perimeter of the system and the extent of applicable security controls to be defined and built in to the system. Figure 1 below[5] shows a simple client-server based system with the security boundary shown in green.

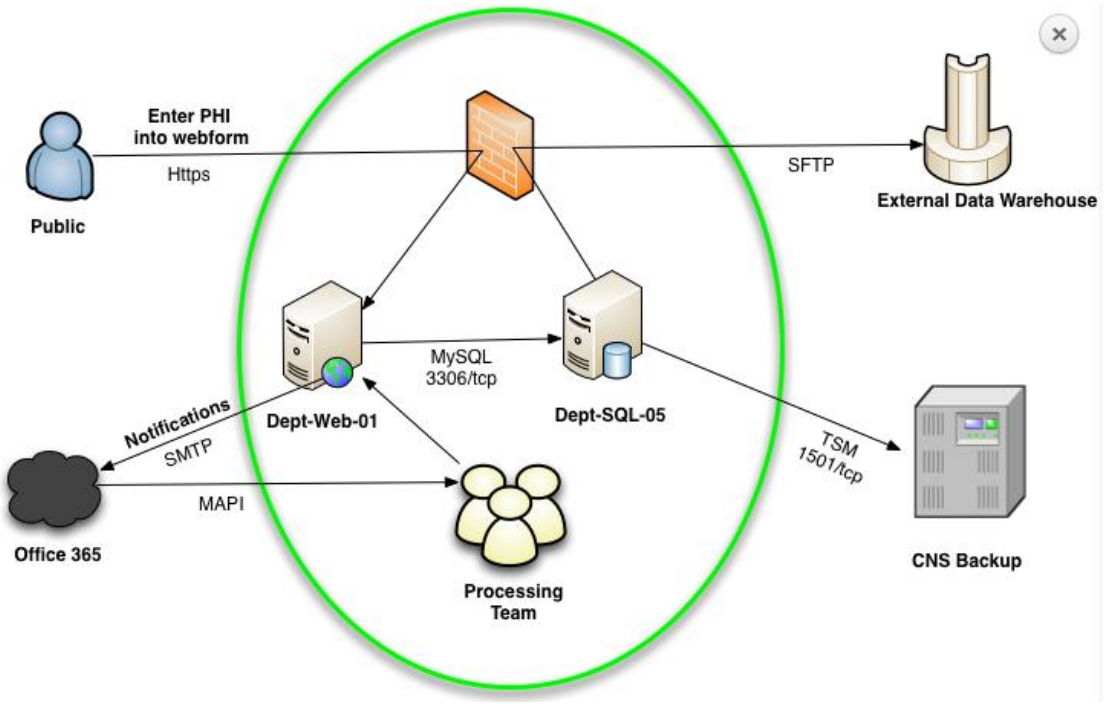

Figure 1: The System Security Boundary

The System Security Plan should address the hardware, software, security controls, and administrative or configuration issues associated with security the system and the data within that boundary. The plan should also describe the interactions with adjacent systems and networks and, where necessary, describe the security controls that protect access and secure the data.

RISK MANAGEMENT FRAMEWORK

The University of Wisconsin-Madison Cybersecurity Risk Management Framework is designed to provide departmental directors and managers, researchers, and information technologists with a tool to determine risk to data and operations of each network or system connected to or serviced by the campus information technology architecture. The Risk Management Framework, also called the RMF, is derived from the National Institute for Standards and Technology Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and specifically tailored to meet the requirements and culture at the University. This section describes the RMF processes and implementation details and serves as a guide to determining cybersecurity risk to information

[4] From NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*, dated May 2013

[5] From University of Florida article *Creating an Information System/Data Flow Diagram* found at https://security.ufl.edu/it-workers/risk-assessment/creating-an-information-systemdata-flow-diagram/

systems and network architectures. The RMF consists of six steps that guide the development of a system with information security controls built in. Once development is completed, a formal risk assessment and continued operating checks ensure maintenance of defined risk levels. The tables and graphic below describe the steps:

Steps within the Risk Management Framework

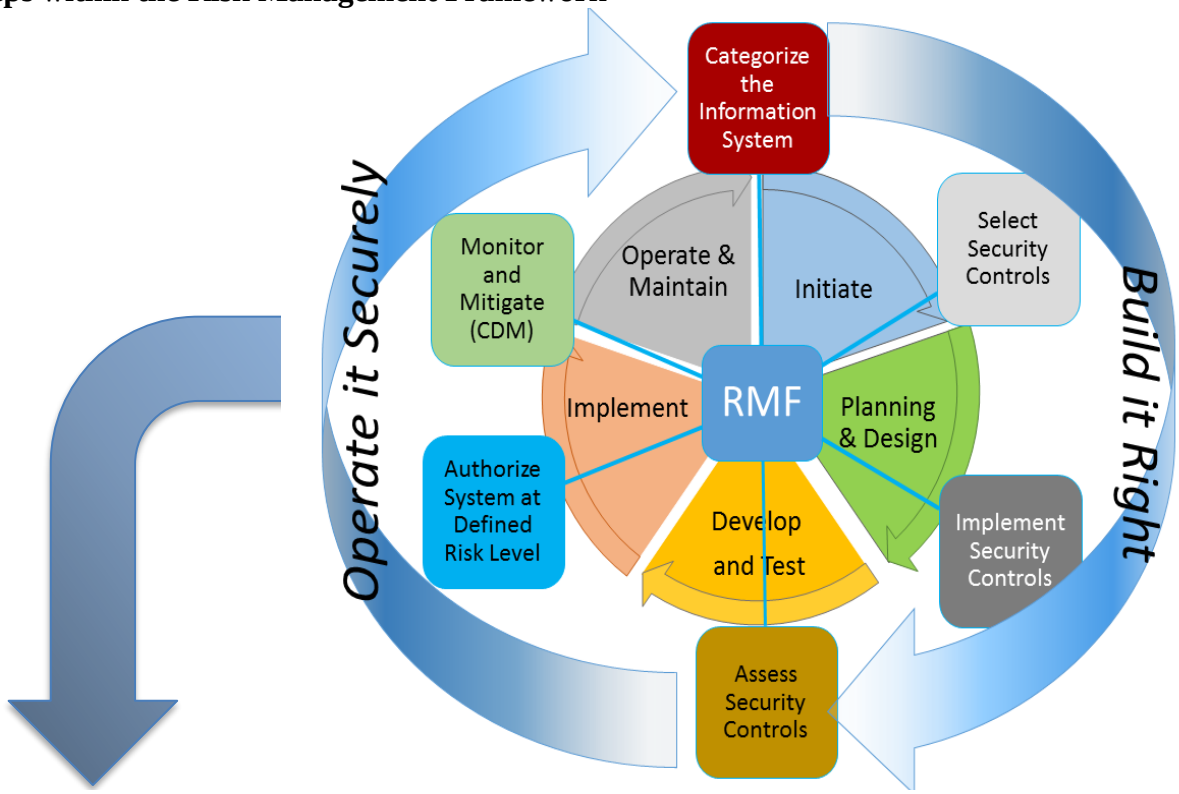

Figure 2: The Risk Management Framework

STEP	ACTIVITY TITLE	DESCRIPTION
PRE	Planning	Conducting discovery with the System Owner to aid in their understanding of the RMF and associated tools and processes. Identification of estimated level of effort, schedule and resources occurs here.
1	Categorize the System	A data driven and collaborative process where the security requirements of the system are defined by the highest classification of data handled by, or stored within, the system or processes. The System Owner must agree with the System Category to move on to the next step.
2	Select Security Controls	Assignment of the administrative, physical and technical controls required to protect the data are drawn from an agreed security controls framework (e.g., NIST 800-53). Alignment with specific compliance programs (i.e., HIPAA, FERPA, EU GDPR, GLBA, etc.) is necessary to ensure accuracy. The proper controls are selected by the Risk Analyst in consultation with the System Owner. Controls that are not attainable will be accompanied by

STEP	ACTIVITY TITLE	DESCRIPTION
		a suitable mitigation or explanation from the System Owner will be recorded.
3	Implement and Validate Controls	During design and development, the System Owner and Developers ensure the selected controls are incorporated in the system design, validated to provide the desired protections, and verified as operational. Consulting services from the Office of Cybersecurity are available as resources allow.
4	Risk Assessment	Independent of the development team, the Office of Cybersecurity conducts a documented assessment to test the selected controls. Residual risk is determined with mitigating factors applied. This stage leads to a formal declaration of risk for the system or network.
5	Authorize the System	A final risk review is conducted with a formal declaration of risk provided by the CISO to the responsible Risk Executive who makes the determination whether to (1) operate the system at the defined risk level; (2) further mitigate risk; or (3) decline to allow continued operation.
	SYSTEM IS OPERATIONAL	
6	Monitor and Mitigate	The System Owner or the Cybersecurity Operations Center should continually assess the operational controls against evolving vulnerability, threat and impact factors. Disruption to operations or loss of data occurs when controls fail, system upgrades occur without proper testing or external factors dictate, determine and implement mitigating controls or return the system to an earlier RMF step. This step is also known as Continuous Diagnostics and Mitigation (CDM).

As shown in the table below, the RMF aligns with the system development life cycle and requires input documentation and information for each step. Output artifacts are produced that are used in planning, development and testing, and certification of risk leading to implementation as shown in the table below.

STEP	ACTIVITY TITLE	PROJECT PHASE	INPUT DOCUMENTS AND ACTIVITIES	OUTPUT DOCUMENTS AND ACTIVITIES
1	Categorize the System	Planning and Design	• Data definition including Classification • FISMA determination from Contract • Data description • System description from SDLC • CIS Benchmarks	• Cybersecurity Project Charter • System Security Plan (SSP) Questionnaire checklist • Data Security Triage Form • IT Security Baseline for Research and Academic Computing Template

STEP	ACTIVITY TITLE	PROJECT PHASE	INPUT DOCUMENTS AND ACTIVITIES	OUTPUT DOCUMENTS AND ACTIVITIES
				• Interview Checklist(s): e.g., FISMA Controls, HIPPA Test Plan, SA Checklist
2	Select Security Controls		• Complete and Validated SSP Questionnaire checklist	• Security Controls Inventory

3	Implement and Validate Controls	Develop and Test	• Configure Security Controls as determined.	• Completed Package Artifacts
				  ○ SSP
				  ○ Topology, Data Flow, System Security Boundary
				  ○ Ports & Protocols Table
				• Security Controls Workbook (Pre-Assessment)
				• Submitted Cybersecurity Risk Acceptance Request Form

4	Risk Assessment		• Provide All Audit Scan (host based scans & application based testing) • Completed Security Controls Checklist validated by scanning and manual review • Develop and Execute Testing Plans (Artifacts not provided will be created by the Office of Cybersecurity) • Step Three Deliverables	• Scanning tool (i.e., Qualys) generated Risk Assessment Report plus Analyst notes • Executed CCI and NIST checklists • Updated systems POAM • Validated Step Three Artifacts • Residual Risk Report
5	Authorize System	Implement	• Residual Risk Report • Step Four deliverables	• Chief Information Security Officer signed Risk Letter plus Risk Executive's Endorsement/Approval to Operate

STEP	ACTIVITY TITLE	PROJECT PHASE	INPUT DOCUMENTS AND ACTIVITIES	OUTPUT DOCUMENTS AND ACTIVITIES
PROJECT HANDOFF TO OPERATIONS				
6	Mitigate and Monitor (CDM)	Operate	• Approved scanning tool • Control Validation Plan • Step Five deliverables	• Provide Monthly Risk Reports & POAM updates • Security Control Validation Report

LEVEL OF EFFORT

The time to complete each step within the RMF depends on the data classification, information system size, and technical complexity. Each system will be assigned a Risk Analyst from the Office of Cybersecurity who will consult with and assist the technical teams, developers, system owners, business process owners, IT managers and Risk Executives in navigating the process. The tables below show a rough estimate of the level of effort for the assigned Risk Analyst for the overall risk assessment effort including all steps in the RMF. Level of effort and time to complete the process should be determined collaboratively at the onset of the project and is the responsibility of the system owner.

The Office of Cybersecurity has limited resources to assist and each engagement would be determined on when assets are available using a "best effort" approach. The table below shows an estimated level of effort based on the type of service needed and the relative size of the information system. This level of effort is contact time with the project only, not calendar hours or days necessary to gather all information, delays due to scheduling challenges, hand off time between reviews, or holiday and weekend hold time. The term "assets" encompasses host terminals, servers, switches, routers, firewalls, intrusion detection or protection systems or peripherals. When defining a system, including all active components that primarily security related is required to properly set the scope of the effort.

SERVICE	SYSTEM SIZE	# ASSETS	LABOR REQUIRED	LOE HOURS
CONSULTING SUPPORT	Small	1 – 5	1 Consultant	40
	Medium	6 – 15	1 Consultant	60
	Large	16 – 50	1 Consultant	60 - 80
	Extra Large	50+	1 Consultant 1 Specialist	120+
CONSULTING AND ASSISTANCE IN DEVELOPING SYSTEM SECURITY PLAN AND ARTIFACTS	Small	1 – 5	1 Consultant	60
	Medium	6-15	1 Consultant	80
	Large	16 – 30	1 Consultant	160
	Extra Large	30+	1 Consultant 1 Specialist	200+
CONSULTANT SUPPORT LABOR WITH SSP ARTIFACTS AND FULL TESTING SUPPORT	Small	1 – 5	1 Consultant 1 Specialist	120
	Medium	6-15	2 Consultants	200
	Large	16 – 50	2 Consultants 1 Specialist	300
	Extra Large	50+	2 Consultant	500+

SERVICE	SYSTEM SIZE	# ASSETS	LABOR REQUIRED	LOE HOURS
			2-3 Specialists	
CYBERSECURITY ARCHITECTURE AND ENGINEERING	Small	1 – 5	1 Consultant 1 Specialist	Project Dependent
	Medium	6-15	2 Consultants	
	Large	16 – 30	2 Consultants 1 Specialist	
	Extra Large	30+	1 Consultant 2+ Specialists	

The time estimated within each step of the RMF is shown in the table below and reflects a rough estimate of calendar days, weeks or months to process through each step given information is available and testing windows can be scheduled. Time to obtain a Risk Executive Signature is wholly dependent on the organization and the System Owner communications with the Risk Executive.

STEP WITHIN RMF	SYSTEM SIZE	ESTIMATED HOURS OR DAYS WITHIN EACH STEP
PLANNING	Small	2 weeks
	Medium	2 weeks
	Large	2 – 3 weeks
	Extra Large	2 – 3 weeks
STEP 1: CATEGORIZE THE SYSTEM	Small	1 day
	Medium	1 day
	Large	1 day
	Extra Large	2 days
STEP 2: SELECT SECURITY CONTROLS	Small	1 day
	Medium	1 day
	Large	2 days
	Extra Large	1 week
STEP 3: IMPLEMENT AND VALIDATE CONTROLS	Small	System Owner and Project Team dependent
	Medium	
	Large	
	Extra Large	
STEP 4: RISK ASSESSMENT	Small	2 days (depending on test duration needed)
	Medium	<5 days (depending on test duration needed)
	Large	1.5-2 weeks (depending on test duration needed)
	Extra Large	>2 weeks (depending on test duration needed)
	Small	<1 day

STEP WITHIN RMF	SYSTEM SIZE	ESTIMATED HOURS OR DAYS WITHIN EACH STEP
STEP 5: AUTHORIZE THE SYSTEM (PRESENTATION AND CISO SIGNATURE	Medium	1 day
	Large	<2 days
	Extra Large	2 days
STEP 5: AUTHORIZE THE SYSTEM (RISK EXECUTIVE SIGNATURE)	Small	<1 day
	Medium	1 day
	Large	<2 days
	Extra Large	2 days

A full description of each service and activities that take place in each step of the RMF along with information on the related cost is available upon request from the Office of Cybersecurity.

SECURITY CONTROL INHERITANCE

For most information systems and applications, there are security controls that can be inherited from the surrounding infrastructure or adjacent business processes or systems within the architecture. System Owners and Risk Executives should consider a security control as "inheritable" if it is a verified security asset. Much like an inheritance receive from the death of a relative, it's not real until it has been verified to exist and is functioning.

Information Systems "**inherit**" controls **from** an architecture or program like a child inherits heirlooms, property or money from a parent. **System owners can allow "inheritance**" of a security control **to** another architecture much as the deceased addressed the disposition of their earthly items in their Last Will and Testament. When an information system allows a control to be "inherited" and used by another system or architecture, the "parent" System Owner is responsible for keeping the control functioning – including making available to the "child" System Owner a record of periodic verification of that control.

Finally, the inherited control has to be appropriate for the system or architecture. For example, inheriting multi-factor authenticator management from the current UW System Human Resources System (HRS) which is using Symantec Multi-factor Authentication (MFA) and applying that control to a research data warehouse system where we want to have Duo MFA in place is, by rote, a control you cannot inherit where inheriting the availability of backup power supplied to a data center can cover a broad group of systems if housed within that data center.

Inherited security controls should be clearly marked within the Risk Assessment Tool and the Plan of Action and Milestones for the information system.

Appendix B – Initial List of Risk Executives

The following is the initial list of University units that should appoint Risk Executives for the Implementation Plan for the University of Wisconsin-Madison Cybersecurity Risk Management Policy. This includes Deans, Directors, and other leaders of high level university divisions and institutes.

A01 General Education Admin
A02 General Services, AIMS
A03 Business Services
A04 Division of Student Life
A05 Enrollment Management
A06 Division of Information Technology (DoIT)
A07 College of Agriculture and Life Sciences
A10 International Division
A12 Wisconsin School of Business
A17 School of Education
A18 Arts Institute
A19 College of Engineering
A27 School of Human Ecology
A34 Vice Chancellor for Research & Graduate Education
A40 Nelson Institute for Environmental Studies
A42 Division of Intercollegiate Athletics
A45 Law School
A48 College of Letters & Sciences
A49 General Library System
A52 Wisconsin State Lab of Hygiene
A53 School of Medicine and Public Health
A54 School of Nursing
A56 School of Pharmacy
A57 University Health Services
A71 Facilities Planning & Management
A77 University of Wisconsin Police
A80 Recreational Sports
A85 University Housing
A87 School of Veterinary Medicine
A88 Wisconsin Veterinary Diagnostic Lab
A93 Division of Continuing Studies
A96 Wisconsin Union

Appendix C – Terms, Definitions and Acronyms

TERMS AND DEFINITIONS

The terms and definitions shown below are provided to clarify specific characteristics of cybersecurity articulated within this document. Reference to source documents are provided as necessary to ensure complete understanding.

Application - A software program hosted by an information system. (NIST SP 800-37r1, Appendix B)

Availability - Ensuring timely and reliable access to and use of information. (44 U.S.C., Sec. 3542)

Authorization (to operate) – The official management decision given by the Risk Executive to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37r1, Appendix B, Adapted)

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (44 U.S.C., Sec. 3542)

Cybersecurity - The ability to protect or defend the use of cyberspace from cyber-attacks (CNSS 4009). Derived from the term "cybernetics" which is the scientific study of communication and control processes in biological, mechanical, and electronic systems and originated from Greek *kubernan* meaning to steer or control (OED).

Data Governance – defined by the implementation of the UW–Madison data management framework, (in progress). For more information contact policy@cio.wisc.edu. For the current presentation on the topic, see:
https://www.cio.wisc.edu/wp-content/uploads/2014/12/DataGovernanceFramework.pptx.

Information Category – As defined in National Institute of Standards and Technology Special Publication 800-60 (NIST SP 800-60 rev 1), *Guide for Mapping Types of Information and Information Systems to Security Categories*; Infomation is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation. UW–Madison information categories are represented on Page 6 of the *Introduction* to this document.

Information Classification – in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for that data.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (See 44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III)

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (44 U.S.C., Sec. 3542)

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (44 U.S.C., Sec. 3542)

Plan of Actions and Milestones (POAM) – A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (OMB Memorandum 02-01)

Risk – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (FIPS 200, Adapted)

Risk Analyst – Individual from the Office of Cybersecurity assigned to help capture and refine information security requirements and ensure their integration into information technology component products and information systems through purposeful security design or configuration. (NIST SP 800-37r1, Appendix B, Adapted)

Risk Assessment – The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations, resulting from the operation of an information system. (NIST SP 800-37r1, Appendix B, Adapted)

Risk Executive – The Risk Executive should be an executive or director, (e.g., Dean or their appointee, department chair, director of a research lab, etc.,) within the academic / functional unit, or in the line of authority above that unit. The Risk Executive must have the authority to accept the risk of operating the system on behalf of the institution and should be in the unit who will ultimately be responsible for paying for a breach (i.e., Dean or their appointee, department, research lab, etc.) (Cybersecurity Risk Management Implementation Plan)

Risk Executive (Function) – An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

Risk Management - The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (FIPS 200, Adapted)

Risk Register – A database managed by the Office of Cybersecurity that contains records for each Information System to which the Risk Management Framework is applied.

Security Category – "The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals." (FIPS 199, Appendix A, p.8)

Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (FIPS 199)

Security Control Inheritance – A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. (NIST SP 800-37r1, Appendix B)

System Owner – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (NIST SP 800-37r1, Appendix B)

System Security Plan – Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. (NIST SP 800-37r1, Appendix B; See: NIST SP 800-18)

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NIST SP 800-37r1, Appendix B, Adapted)

Threat Source – The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent. (NIST SP 800-37r1, Appendix B)

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST SP 800-37r1, Appendix B)

ACRONYMS AND ABBREVIATIONS

The table below provides the long title associated with acronyms or abbreviations used in this document.

Acronym or Abbreviation	Long Title
D-CISO	Deputy Chief Information Security Officer
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DoIT	Division of Information Technology
FERPA	Family Educational Rights and Privacy Act of 1974
HCC	Health Care Component
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HRS	Human Resource System
IRB	Institutional Review Boards
ITC	Information Technology Council
MIST	Madison Information Security Team
NIST	National Institute for Standards and Technology
NIST SP	NIST Special Publication
PCI-DSS	Payment Card Industry Data Security Standard
PHI	Personal Healthcare Information
PII	Personally Identifiable Information
PAT	Policy Analysis Team
POAM	Plan of Actions and Milestones
RMF	Risk Management Framework
SDLC	Systems Development Life Cycle
SETA	Security Education, Training & Awareness
SFS	Shared Financial System
UW–Madison	University of Wisconsin–Madison
UWSA	University of Wisconsin System Administration
VCFA	Vice Chancellor for Finance and Administration
VP IT	Vice Provost for Information Technology

FACULTY SENATE
MINUTES
05 March 2018

Chancellor Rebecca Blank called the meeting to order at 3:32 p.m. with 136 voting members present (109 needed for quorum). Chancellor Blank reported on the addition of public broadcasting to the parts of UW Extension that are returning to Madison, Bucky's Tuition Promise, several high-level searches, campus events during Black History Month, and final statistics on undergraduate applications. Vice Provost and Chief Diversity Officer Patrick Sims presented the annual State of Diversity and Inclusion address. There was a question for Vice Provost Sims about what faculty can do to address diversity, a question for Chancellor Blank on graduate student fee structure, a question directed to both about diversity in undergraduate applications, and a statement commending the campus position on high school protests. The minutes of the meeting of February 5, 2018, were approved.

Employee Assistance Office Director Sherry Boeger presented the annual reports for the Ombuds Office (Faculty Document 2726) and the Employee Assistance Office (Faculty Document 2727). There was one question about the handling of graduate student visitors, to which Ombud and Professor Emeritus Chuck Snowden responded.

Professor Anja Wanner (University Committee, District 120) presented Faculty Document 2728, which proposes modifications to the charge of the Campus Diversity and Climate Committee (CDCC), for a first reading. The current CDCC charge reflects a time before the Division of Diversity, Equity, & Educational Achievement (DDEEA) was created as the administrative office for diversity and inclusion on campus; the proposed changes are intended to make the CDCC parallel other shared governance committees. Professor Wanner presented Faculty Document 2729, which proposes the creation of a new committee addressing access and accommodation, for a first reading. The new Committee on Disability Access and Inclusion (CDAI) would roll together the functions of a number of other committees, expand and rationalize their charge, and connect shared governance with the campus ADA Coordinator in the Office of Compliance. There were no questions or comments on either first reading.

Associate Professor Noah Weeth Feinstein (Community & Environmental Sociology, District 18) and member, Committee on Committees) presented the report on nominations for election to the divisional committees and the Graduate Faculty Executive Committee (GFEC) (Faculty Document 2730). Chancellor Blank noted that Prof. Feinstein's report, combined with his report from the previous Senate meeting (Faculty Document 2722), constitute the full slates for election this year. She called for nominations from the floor and received none. Prof. Wanner presented information on senate electoral districts (Faculty Document 2731), noting that the new apportionment combines two districts to reflect the merger of Landscape Architecture and Urban & Regional Planning into Planning & Landscape Architecture (District 22), moves History of Science from its old district with Medical History & Bioethics and folds it into History (District 60), and increases the overall number of senators by one.

Professor Wanner presented a proposal to clarify the language of *FPP* 3.05.H. regarding the role of academic staff on graduate student committees (Faculty Document 2700) for a first reading. There were two comments, which will be considered prior to this item being brought up for a vote. Professor Chad Goldberg (Sociology, District 71) moved to suspend the orders of the day and immediately take up agenda item 14. The motion was seconded and passed by voice vote. Prof. Goldberg moved adoption of Faculty Document 2734, a resolution calling on President Ray Cross to reaffirm commitment to shared governance. The motion was seconded. Professor Ruth Litovsky (University Committee, District 120) moved modification of the second clause of the resolution as follows:

> WHEREAS ~~a history of repeated injuries impelled~~ the UW-Madison Faculty Senate on May 2, 2016, ~~to~~ declared no confidence in President Cross and the Board of Regents and ~~to~~ called on them to "recommit themselves to the Wisconsin Idea" by "working with us to strengthen the quality of our state universities," which led to an unprecedented wave of no-confidence votes across the UW System;

The amendment passed by voice vote. Prof. Litovsky moved modification of the "resolved" clause as follows.

> BE IT RESOLVED THAT the Faculty Senate of the University of Wisconsin-Madison hereby ~~demands~~ expects ~~that~~ President Cross to honor his earlier pledge to protect and respect shared governance in all relevant administrative decisions regarding the UW System and its campuses, and that he outline specific policies and practices for including faculty, staff, and students in meaningful shared governance at the System level, in a manner that respects and supports the contributions of all members of the University of Wisconsin System in guiding its decisions.

Following a couple of objections to the word "expects," Prof. Litovsky modified her amendment to replace "expects" with "calls upon." There was no objection to this change, which was thus adopted by consent. There was one comment against the amendment. The amendment passed by a show of hands. Professor Thomas O'Guinn (Business, District 24) moved adoption of a second "resolved" clause as follows.

> BE IT FURTHER RESOLVED that we call on UW-Madison faculty to uphold our right to shared governance, and affirm our duty to speak, act, and govern.

The motion was seconded. Assistant Professor Peter Adamczyk (Mechanical Engineering, District 39) proposed changing "we call" to "the Faculty Senate calls." There was no objection to this change, which was thus adopted by consent. The amendment passed by voice vote. The resolution as amended passed by voice vote.

Prof. Wanner moved adoption of Faculty Document 2723, which makes several changes to *Faculty Policies & Procedures* Chapter 4 intended to clarify and simplify divisional membership, bring *FPP* in line with practice on some points, and modify practice on other points, for a first reading. The motion passed by voice vote. Prof. Wanner presented Faculty Document 2732, a proposal to make the chancellor's Advisory Council on Immigration and International Student Issues into a standing shared governance committee for student and staff, for a first reading. The chair of the advisory committee, Associate Professor Cindy I-Fen Cheng (History) spoke to the proposal. Prof. Wanner presented Faculty Document 2733, which contains a number of updates and clarifications to *FPP* Chapter 6, for a first reading. There were several comments, which will be incorporated into the document prior to a vote next month.

Chancellor Blank adjourned the meeting at 4:54 p.m.

Steven K. Smith
Secretary of the Faculty

Recommended changes to Campus Diversity and Climate Committee (CDCC)
***Faculty Policies and Procedures* 6.27.**

Over the course of the last few semesters, the University Committee, the Secretary of the Faculty, the chair and members of the CDCC, the staff of the DDEEA, and university leadership have been discussing updating the charge of the CDCC. There are several reasons for the resulting proposal below, among which are:

- The CDCC predates the office of the Chief Diversity Officer. Thus there are parts of the committee's charge that directly relate to functions now performed by DDEEA. Several of the proposed changes below are in recognition of the fact that some of the current CDCC functions are not exercised by any other shared governance committee. These functions are more efficiently and appropriately housed in an administrative office rather than in a shared governance committee, the role of which is more advice, oversight, and input, rather than execution of administrative functions.

- As a result of this long history, the CDCC has grown to include up to 20 ex officio members, creating an unwieldy and unnecessarily complicated body. All committee are free to invite guests or otherwise work with people outside the committee, without the need for an official "consultant" designation, so this has been removed in the proposal below.

- The Advisory Committee for the Office of Equity and Diversity is focused on advising that office with regards to a compliance function that has been moved to the Office of Compliance. Some of the changes below are to incorporate some of the functions of the Advisory Committee to the OED. (A new committee, the CDAI, considered separately, will include the remaining charge of this committee, which would be retired if the new committee and the changes below are approved.)

The CDCC issued a report in August 2017 outlining changes to FPP that it felt improved the functionality of the committee. These included reducing the number of CDCC functions from twelve to seven by eliminating functions that are outdated, duplicative, confusing, or exceed CDCC resources and also developing a subcommittee structure to make better use of CDCC members' time and talents and facilitate CDCC performance of its functions.

The August 2017 document proposed four subcommittees, rather than the three below. The one that is not included in the proposal below is a "chancellor-provost meetings" subcommittee. One of the changes proposed below that was not part of the August 2017 CDCC document is the elimination of the twice annual meetings with the chancellor and provost. These meetings, like the CDCC itself, predate the creation of the office of the vice provost and chief diversity officer. Eliminating these meetings brings this committee into line with other Chapter 6 committees and makes this particular subcommittee unnecessary.

Two elements of the proposal below are specifically aimed at strengthening and focusing the CDCC's role as supportive of the DDEEA and diversity and inclusion more generally:

- The preamble to the functions of the committee have been edited to include the Institutional Statement on Diversity, which was a product of cross-campus input approved by the Faculty Senate and other governance bodies.
- The function that is now listed first was moved up from the sixth position, emphasizing that the CDCC works **with** the office of the chief diversity officer.

(continued)

6.27. CAMPUS DIVERSITY AND CLIMATE COMMITTEE.

A. MEMBERSHIP.

1. Four faculty ~~chosen as specified by FP&P §6.05~~.
2. Four academic staff ~~chosen as specified by FP&P~~ ~~§6.05~~.
3. Four students ~~chosen as specified by FP&P~~ ~~§6.05~~.
4. Four university staff ~~appointed by FP&P~~ ~~§6.05~~.
5. Two alumni appointed by the chancellor after consultation with the Wisconsin Alumni Association.
6. Two community representatives appointed by the chancellor.
7. The Vice Provost for Diversity and Climate/Chief Diversity Officer, ex officio nonvoting.
8. ~~The chancellor or provost may appoint ex officio nonvoting members, or the committee may appoint consultants, to ensure effective coordination by the CDCC with other FP&P shared governance committees and campus units focused on issues of diversity and climate~~.
9. Faculty, staff, alumni, and community representatives appointed under A.1, A.2, A.4., A.5., and A.6. shall serve three-year staggered terms, and may be reappointed to second consecutive three-year terms. Students selected under A.3. shall serve renewable one-year terms.
10. The committee shall elect two co-chairs. One co-chair shall be elected from among the faculty members appointed pursuant to Section A.1. The second co-chair shall be elected among the other shared governance groups appointed pursuant to Section A.2, A.3, and A.4.

B. **FUNCTIONS**

This shared governance body advises the administration, ~~the~~ faculty, ~~the~~ staff, and ~~the recognized~~ student<u>s</u> ~~governance organization~~ on campus diversity and climate<u>, which as noted in the UW-Madison Institutional Statement on Diversity, is a source of strength, creativity, and innovation for this campus. The CDCC values the contributions of each person and respects the profound ways their identity, culture, background, experience, status, abilities, and opinion enrich the university community. As part of that community, the CDCC is committed to the pursuit of excellence in teaching, research, outreach, and diversity as inextricably linked goals.</u> ~~policy, which strives to create an environment where each individual feels respected, valued and supported, while respecting academic freedom and freedom of speech~~.

1. Works collaboratively with <u>and advises</u> the Vice Provost for Diversity and Climate/Chief Diversity Officer to provide direction and accountability for the implementation of university diversity plans.
2. Provides for faculty, staff and student participation in long-range planning <u>and serves as a gateway of information to and from shared governance communities.</u>
3. <u>Reviews campus committees pursuing discrimination goals regarding missions and coordination</u>.
4. <u>Meets with campus leadership to discuss policy and progress on climate and diversity</u>.
5. ~~Meets twice annually with the chancellor and provost to discuss policy and progress~~. ~~Hears periodic reports from the Vice Provost for Diversity and Climate/Chief Diversity Officer on the various initiatives undertaken by his/her office. Hears reports from groups, units, programs and administrators.~~
6. Works with the Office of the Vice Provost for Diversity and Climate/Chief Diversity Officer to plan the annual campus-wide policy and progress forum.
7. Makes policy recommendations.
8. ~~Assists the administration in the preparation of annual reports to the UW System~~.
9. Reports annually to the Faculty Senate, Academic Staff Assembly, ~~the recognized classified staff governance body~~ <u>University Staff Congress</u>, and the current student governance body.
10. Provides updated reports to all shared governance groups of the students, staff, faculty, and to the general public.
11. ~~Meets periodically with deans and directors to discuss policy and progress.~~
12. ~~Coordinates the development of all campus wide diversity plans with specific attention to assessment and resources~~

(continued)

No markup

6.27. CAMPUS DIVERSITY AND CLIMATE COMMITTEE.

A. MEMBERSHIP

1. Four faculty.
2. Four academic staff
3. Four students
4. Four university staff
5. Two alumni appointed by the chancellor after consultation with the Wisconsin Alumni Association.
6. Two community representatives appointed by the chancellor.
7. The Vice Provost for Diversity and Climate/Chief Diversity Officer, ex officio nonvoting.
8. Faculty, staff, alumni, and community representatives appointed under A.1, A.2, A.4., A.5., and A.6. shall serve three-year staggered terms, and may be reappointed to second consecutive three-year terms. Students selected under A.3. shall serve renewable one-year terms.
9. The committee shall elect two co-chairs. One co-chair shall be elected from among the faculty members appointed pursuant to Section A.1. The second co-chair shall be elected among the other shared governance groups appointed pursuant to Section A.2, A.3, and A.4.

B. **FUNCTIONS**

1. This shared governance body advises the administration, faculty, staff, and students on campus diversity and climate, which as noted in the UW-Madison Institutional Statement on Diversity, is a source of strength, creativity, and innovation for this campus. The CDCC values the contributions of each person and respects the profound ways their identity, culture, background, experience, status, abilities, and opinion enrich the university community. As part of that community, the CDCC is committed to the pursuit of excellence in teaching, research, outreach, and diversity as inextricably linked goals.
2. Works collaboratively with and advises the Vice Provost for Diversity and Climate/Chief Diversity Officer to provide direction and accountability for the implementation of university diversity plans.
3. Provides for faculty, staff and student participation in long-range planning and serves as a gateway of information to and from shared governance communities.
4. Reviews campus committees pursuing discrimination goals regarding missions and coordination.
5. Meets with campus leadership to discuss policy and progress on climate and diversity.
6. Works with the Office of the Vice Provost for Diversity and Climate/Chief Diversity Officer to plan the annual campus-wide policy and progress forum.
7. Makes policy recommendations.
8. Reports annually to the Faculty Senate, Academic Staff Assembly, University Staff Congress, and the current student governance body.
9. Provides updated reports to all shared governance groups of the students, staff, faculty, and to the general public.

Proposal to Create the Committee on Disability Access and Inclusion (CDAI) *Faculty Policies and Procedures* 6.31.

There are currently several groups that work with issues of accommodation, accessibility, and inclusion on campus, including governance committees such as the Disability Accommodation Advisory Committee (DAAC; *FPP* 6.33.), the Advisory Committee for the Office for Equity and Diversity (OED) (*FPP* 6.22.), the Committee on Access and Accommodation in Instruction (CAAI), and the Provost's Accessibility and Usability Committee, as well as offices and programs responsible for ADA compliance such as the McBurney Center, OED, FP&M, and of course the ADA Coordinator located within the Office of Compliance in the Office of Legal Affairs. In addition, DoIT is in the process of finalizing a staffing proposal to support access in the web and digital environment and OED will gain a position to work on employee accommodations.

The proposal below focuses the work of these various bodies into one shared governance committee to provide advice to leadership and the campus on accessibility matters and advocate for the diverse needs of the disability community at UW-Madison. It further connects that single committee to the ADA Coordinator, while maintaining the various links across campus to others who work with these issues. This proposal was developed by Cathy Trueba, Director of Compliance and the current campus ADA Coordinator, in consultation with the Secretary of the Faculty. It is based on the charges for the existing committees mentioned above, modified to reflect current campus needs in this area, with substantial input from current and past members of those bodies and other stakeholders.

FPP 6.31. –COMMITTEE ON DISABILITY ACCESS AND INCLUSION

A. MEMBERSHIP.
   1. Three faculty
   2. Two academic staff
   3. Two university staff
   4. Two students (one undergraduate and one graduate or professional school student)
   5. ADA Coordinator (Ex Officio voting)
   6. McBurney Disability Resource Director (Ex Officio voting)
   7. Office for Equity and Diversity Disability Coordinator/Employment (Ex Officio voting)
   8. Facilities, Planning and Management Accessibility Specialist (Ex Officio voting)
   9. Digital Technology Accessibility (Associate) Director(Ex Officio voting)

   The committee relies on expertise from a variety of offices that work in the area of access and accommodation, including but not limited by enumeration to: Athletics; Division of Diversity, Equity and Educational Achievement; Division of Student Life; Libraries; Office of Admissions and Recruitment; Office of Human Resources; Office of Legal Affairs; Recreational Sports; Teaching Academy; Transportation Services; Undergraduate Advising; University Health Services; University Housing; University Marketing; Vice Chancellor for Research and Graduate Education/Graduate School; Wisconsin Union.

(continued)

The committee shall select its own chair from among the faculty members on the committee. The committee may select a co-chair from among the other voting, non-ex officio members. Terms of faculty and staff members shall be three years; terms of student appointees shall be one year. Each committee member will serve on the main committee and at least one subcommittee.

B. FUNCTIONS

1. Advise the University ADA Coordinator and relevant institutional units with primary responsibility for ADA compliance, and support their work to ensure the policies, programs, and services of the institution are accessible for students, employees, and guests of the university who have disabilities.
2. Guide or contribute to assessment outcomes leading to improvements in the campus experience.
3. Promote educational activities that support an inclusive campus community and compliance with laws relating to individuals with disabilities.
4. Review applicable policies and practices. Recommend new policies, practices, or changes to existing policies or practices to campus governance bodies or institutional leaders, as appropriate.
5. Lead and/or participate in university initiatives designed to measure campus climate, increase the diversity of the campus community, and improve the experiences of people with disabilities.

C. SUBCOMMITTEE ON INSTRUCTIONAL ACCESS

Instructional access includes but is not limited to classroom, laboratory, internship, externship, study abroad and field experiences; admission and application processes; grading; curriculum requirements.

1. Membership:
   a. One faculty (co-chair)
   b. Two academic staff
   c. One student
   d. McBurney Director (co-chair)
   e. Division of Student Life representative
   f. Digital Technology Accessibility (Associate) Director
   g. Libraries representative
   h. Office of Admissions and Recruitment representative
   i. Teaching Academy representative
   j. University Health Services representative
   k. Vice Chancellor for Research and Graduate Education or designee

2. Functions
   a. Review policies and procedures and recommend changes to ensure the instructional environment is accessible to students with disabilities.
   b. Develop and/or recommend best practices and training for instructors on accessible and inclusive instructional design.
   c. Serve as the first level appellate body for the denial of an academic or instructional accommodation where there is no existing internal appeal or grievance process.

D. SUBCOMMITTEE ON EMPLOYMENT ACCESS

Employment Access includes but is not limited to matters concerning the recruitment and retention of employees with disabilities, policies regarding the provision of reasonable accommodations in the workplace, and education and training regarding workforce members with disabilities.

1. Membership:
    a. One faculty (co-chair)
    b. One university staff
    c. Office for Equity and Diversity Disability Coordinator/Employment (co-chair)
    d. Facilities, Planning and Management Accessibility Specialist
    e. Division of Diversity, Equity and Educational Achievement representative
    f. Office of Human Resources representative
    g. Office of Legal Affairs representative
    h. UW Marketing representative

E. SUBCOMMITTEE ON PHYSICAL AND DIGITAL ACCESS

Physical and technology access includes but is not limited to ensuring that the physical and digital environment and processes that underlie these environments (i.e., procurement, training, utilization policies, etc.) are accessible to students, employees, and visitors with disabilities.

1. Membership:
    a. One faculty (co-chair)
    b. One academic or university staff
    c. One student
    d. McBurney Disability Resource Director or designee
    e. Facilities, Planning and Management Accessibility Specialist
    f. Digital Technology Accessibility (Associate) Director (co-chair)
    g. Libraries representative
    h. Recreational Sports representative
    i. Athletics representative
    j. Transportation Services representative
    k. Housing representative
    l. Wisconsin Union representative
    m. UW Marketing representative
    n. UWPD representative

Proposed updates to *Faculty Policies and Procedures:* 6.01., 6.02., 6.03., 6.04., 6.07., 6.09., 6.10., 6.11., 6.12., and 6.49.

Most of FPP Chapter 6 lists and describes the various shared governance committees. The first several sections of the chapter, however, deal with "meta" information about all shared governance committees. The changes proposed below all relate to those introductory sections. On the first reading of these proposed changes at the March 5, 2018, Faculty Senate meeting, some concern was expressed about the lumping together of various changes. Thus the changes have been formatted differently here to better reflect what is being proposed and the reasons behind the proposed changes. In general, the proposal reorganizes the introductory sections thematically, clarifies roles, changes the word "joint" to "shared," and adjusts "classified" staff to "university" staff. One specific change to note is that this proposal moves search and screen committees out of the listing of individual committees and instead includes them in the section on "types" of committees. In addition, we have proposed language to clarify and reiterate the role of shared governance in these committees. (New language is underlined and deleted language is ~~crossed off~~. *Italics* indicates a change arising from or after the first reading.)

To see these changes to Chapter 6 with no mark-up and in full context, see the Office of the Secretary of the Faculty KB: https://kb.wisc.edu/sof/page.php?id=81159

Proposed Language	**Explanation**
6.01.F. The faculty or Faculty Senate*, or the University Committee or other authorized appointing body*, may provide for the selection of committee members; the scope of their authority; the rules and regulations for their proceedings; and the form in which the committee's work should be reported	- Specifies that the University Committee, as the executive committee of the Senate, is responsible on a day-to-day basis for oversight of the overall committee structure. - Reflects that the University Committee operates at the direction of the Faculty Senate. - Acknowledges that there are several bodies that appoint committees.
6.01.G. Ad hoc faculty committees established by the faculty, University Committee, or Faculty Senate are subject to the general provisions of this chapter	- Reflects that both the Faculty Senate itself and the University Committee as its executive committee appoint ad hoc committees.
6.02. ~~JOINT~~ SHARED GOVERNANCE COMMITTEES. A. "~~Joint~~ Shared governance committees" are committees established in conjunction with academic staff~~, classified~~ university staff, and/or student government to address issues of common concern which are not the primary responsibility of the faculty. B. A ~~joint~~ shared governance committee reports to the faculty through the University Committee and/or the Faculty Senate and to other establishing authorities in accordance with their rules.	- Governance involving more than one of the governance groups has been referred to as "shared governance" for some time. - Moreover, "joint governance" leads to confusion with the joint governance appointments covered in Chapter 5. - In 2015, "classified staff" became "university staff."

(continued)

6.03. ADVISORY COMMITTEES An Advisory Committee is any committee or work group whose purpose is to provide advice on a specific issue or topic to the convener of the committee/work group. The purpose and intent of an Advisory Committee is dictated by and at the control of the appointing body that established the committee/work group. The person/department that convened the committee/work group controls the membership and the process for establishing membership. Advisory Committees can be for any period of time.	- The current section 6.03. ("OTHER COMMITTEES ESTABLISHED BY THE FACULTY") has been moved into section 6.04. below. - This section on "ADVISORY COMMITTEES" is new and was created to reflect the fact that this type of committee is common and follows different rules than other Chapter 6 committees.
6.04. OTHER COMMITTEES ~~CONCERNED WITH ACADEMIC AND EDUCATIONAL ACTIVITIES~~ ESTABLISHED BY THE FACULTY. A. The faculty, University Committee, or ~~the~~ Faculty Senate may establish committees that are not faculty committees as defined in 6.01. or ~~joint~~ shared governance committees as defined in 6.02. All committees established in this chapter shall be referred to as Chapter 6 committees. B. When a committee established by the faculty, University Committee, or ~~the~~ Faculty Senate that is not subject to the provisions of 6.01. considers issues related to academic matters, decisions shall be restricted to a subcommittee consisting of the faculty members of the committee. Decisions of the faculty subcommittee about academic matters cannot be overturned by the full committee. Disputes about identifying issues as academic shall be resolved by the University Committee.	- Section 6.04. as proposed combines the current 6.03. ("OTHER COMMITTEES ESTABLISHED BY THE FACULTY"), 6.04. ("OTHER COMMITTEES CONCERNED WITH ACADEMIC AND EDUCATIONAL ACTIVITIES"), and 6.49. ("SEARCH AND SCREEN COMMITTEES"). The proposed 6.04.A. was formerly 6.03.A. and the proposed 6.04.B. was formerly 6.03.B. - This recognizes that the University Committee, as the executive committee of the Faculty Senate, also establishes committees. - Governance involving more than one governance group has been called "shared governance" for some time. And "joint governance" leads to confusion with appointments covered in Chapter 5.
C. Ad Hoc Committees are working groups established to focus on a targeted purpose for a set duration of time. *If the objectives and responsibilities of an ad hoc committee affect one or more shared governance groups, the appointing authority shall apply shared governance principles to the membership and functions of the committee. To ensure observance of shared governance principles, the appointing authority shall consult with the relevant governance group(s) prior to charging or appointing any ad hoc committees. Disputes as to whether an ad hoc committee should be deemed to be shared governance in scope shall be resolved by the University Committee, after appropriate consultation with the Academic Staff Executive Committee, the Central Committee, and/or Associated Students of Madison.*	- This section is new and intended to ensure that shared governance principles are observed appropriately.

D. Search and Screen Committees are a specific subset of Ad Hoc Committees. Search and Screen Committees are formed for the targeted purpose of hiring a specific position and are charged by the hiring authority. *Search and Screen Committees shall observe the shared governance principles related to the position being recruited. Positions with broad university authority shall follow full shared governance principles as a result, as expressed in the previous section.* 1.~~A.~~ MEMBERSHIP. When a vacancy occurs or is anticipated in the position of academic vice chancellor/provost or at the level of college/school dean a search and screen committee shall be appointed by the chancellor *or authorized hiring authority* and shall consist of: a. ~~1.~~ A faculty majority, as defined in 6.01.C., appointed after consultation with the University Committee. b. ~~2.~~ Administrators, academic staff, ~~classified~~ university staff, and students. c. ~~3.~~ A chair designated by the chancellor from among the faculty majority. 2. ~~B.~~ FUNCTIONS. It is the function of the committee to determine and supply to the chancellor *or authorized hiring authority* an unranked list of acceptable candidates for the vacant position. It is not necessary that the committee ascertain whether each candidate on the list would accept the position if it were offered. *Upon request, the* ~~The~~ committee shall also report to the chancellor *or authorized hiring authority* and *to* the University Committee on the manner in which it conducted its deliberations. 3. ~~C.~~ FURTHER ACTIONS. If none of the slate of candidates recommended is acceptable to the chancellor *or authorized hiring authority* and the Board of Regents, or if all acceptable candidates decline, the committee may be requested to submit a new list of acceptable candidates, or a new search and screen committee may be appointed. [Procedures for the selection of the chancellor conform to Regent policy.]	- This section is adapted from the current FPP 6.49. It is moved here to recognize that Search and Screen Committees are a type of committee, not a specific committee. The revised language is intended to ensure that shared governance principles are observed for all high-level searches, as appropriate. - The inclusion of "or at the level of" under membership reflects the fact that the belief that all academic positions at the level of dean (such as the director of an academic institute or of the libraries) should be subject to the provisions of this chapter. - The inclusion of "or authorized hiring authority" recognizes that the chancellor is not the only office that acts as hiring authority in these situations. - "Classified staff" are now called "university staff."
E. Committees concerned with Academic and Educational Activities. 1. Appropriate faculty bodies shall be consulted before other committees concerned with academic and educational activities are established. The appropriate body for campus-level consultation is the University Committee, and the appropriate bodies for school- and college-level consultation are the school or college academic planning councils.	- This section was moved from FPP 6.03.

2. Faculty members serving on campus-level committees established under the provisions of 6.04.~~A.~~E. should be selected in consultation with the Committee on Committees or the University Committee. 3. Such committees should not normally be established if there is a faculty committee or a committee established by the faculty whose responsibilities cover the academic and educational matters of concern.	
6.06.F. Elections are managed electronically. ~~Election is by ballot distributed to all members of the faculty. Ballots are to be collected at the senate meeting at which the election is scheduled, or delivered to the secretary of the faculty within four days after the meeting.~~	- FPP 6.06. ("ELECTION OF FACULTY TO COMMITTEES") section F as written relates to paper balloting and has been replaced to acknowledge that it is 2018 and elections have been managed electronically for many years. - FPP 6.06.G. and 6.06.H. have been moved to FPP 6.07. below.
6.07. TERMS OF OFFICE. A. With the exception of the University Committee or ~~U~~unless otherwise specified, faculty committee members serve during the academic year ~~one year terms and assume their duties on June 1 following their election~~. ~~B. Appointed faculty committee members serve from the date specified by the appointing authority until the appointing authority has designated a successor. If Faculty Policies and Procedures or faculty legislation establishing a committee specifies a term for an appointment, the.~~ The appointing authority may extend the specified term for one year to avoid too great a turnover of committee members in a single year or to facilitate work in progress. E. A vacancy in an elective committee position is to be reported by the chair of that committee to the secretary of the faculty. F. If circumstances warrant, and upon consultation with the committee concerned, the University Committee shall appoint an appropriately qualified replacement to fill the vacancy until a faculty member is elected at the next annual election to complete the unexpired term. The Committee on Committees will provide input if the vacancy is for the University Committee.	- 6.07.A.: In practice, the only committee that conformed to the terms of this clause was the University Committee (which meets year-round and members assume their duties on June 1). Under each committee, the term lengths are specified. None of these are one-year terms and thus the proposed deletion was unnecessary language. - 6.07.B.: Appointment terms and start and end dates are specified in the charge to every committee, or under the terms of 6.07.A., making much of this language unnecessary/redundant. - 6.07.C. and D. not included here as no changes are proposed. - Proposed 6.07.E. is moved from 6.06.G. - Proposed 6.07.F. is moved from 6.06.H., except for the last sentence, which is new.

6.09. COMMITTEE REPORTS, RECORDS, RECOMMENDATIONS, AND POLICIES. ~~C. If a committee makes a recommendation or proposes a resolution for action by the Faculty Senate, the vote of the faculty members on the committee on the recommendation or proposed resolution shall be reported to the Faculty Senate along with the total committee vote.~~ C. A committee may seek changes to its charge by presenting a proposal to the University Committee.	6.09.C.: It has not been practice to separate out faculty votes from overall committee votes. As long as the provisions for required faculty majorities on academic matters are observed, separating out individual votes from the committee total seems to run counter to voter confidentiality.
6.09.D. Chapter 6 committees shall maintain a written statement of policies and procedures. ~~A committee shall report any proposed changes to these policies and procedures and any contemplated action that would be an exception to these policies and procedures to the University Committee and the chancellor.~~	- Committees maintain their own statements of policies and procedures and are not required to submit them to the UC or to the chancellor. Requiring them to submit any changes to documents that were not submitted previously is pointless.
(6.09.)~~E. If a matter has been reported to the University Committee under the provision of 6.09.D. and if the University Committee so requests, the committee shall postpone action or implementation relating to the matter pending consideration and action by the University Committee and, if the University Committee so decides, by the Faculty Senate.~~	- This is unnecessary. As noted above, committees maintain their own policies and procedures. If these are ever deemed in violation of some other policy, the University Committee and/or Faculty Senate are free to act without need for this clause.
6.10. MEETINGS. A. A faculty committee meets at the call of its chair. A meeting ~~shall be called at the request of any three members of the committee~~ may also be called at the request of a simple majority of members of the committee. B. Faculty should be familiar with and follow the university's open meetings and open records policies, which will also be communicated to committee chairs as part of the committee confirmation letter. C. Meeting agendas should be prepared and distributed in a timely manner by the chair (in conjunction with any committee staff assigned to the committee). Specific rules governing meeting agendas will be communicated to the chair as part of the committee appointment letter. D. Quorum rule: For the purposes of this chapter, a quorum exists when a majority of the voting members of a committee is present. E. Minutes: Will be taken and retained for the meetings of all committees. Guidelines for minutes will be included in committee appointment letters to chairs. Outgoing chairs should give committee documents to the Office of the Secretary of the Faculty to pass on to the next chair or for archiving.	- 6.10. used to consist solely of the first two sentences under what is proposed as "A." ("A faculty committee meets at the call of its chair. A meeting shall be called at the request of any three members of the committee.") The "three members" requirement was changed to "simple majority" to reflect that committees are of widely varying sizes and the simple majority is more consistent with parliamentary practice. - Section D. was moved from 6.11. (and 6.11 is proposed to be deleted). - Sections B, C, and E are new and intended to specify expectations of committee members. This information used to be communicated solely through administrative and appointment letters.

Retirement of the Advisory Committee for the Office for Equity and Diversity (OED), the Disabilities Accommodation Advisory Committee (DAAC), and the Committee on Access and Accommodation in Instruction (CAAI)

Proposed changes to the Campus Diversity and Climate Committee (CDCC, *Faculty Policies and Procedures* 6.27.) and the proposed charge of the new Committee on Disability Access and Inclusion (CDAI, *Faculty Policies and Procedures* 6.31.) absorb the charges of the Advisory Committee for the Office for Equity and Diversity (OED, *Faculty Policies and Procedures* 6.22.), the Disabilities Accommodation Advisory Committee (DAAC, *Faculty Policies and Procedures* 6.33.), and the Committee on Access and Accommodation in Instruction (CAAI). Therefore, the latter three committees are hereby disbanded and the OED and DAAC committees are hereby removed from Faculty Policies and Procedures.

Proposed changes to Faculty Policies and Procedures Chapter 7 based on the report from the Ad Hoc Committee on 7th-year Reviews

The ad hoc committee on 7th year reviews, charged last fall by the University Committee, has issued its final report, based on which the University Committee proposes some changes to FPP Chapter 7. The report is below, followed by the proposed changes.

Final Report of the Ad Hoc Committee on 7th-Year Reviews

This document represents the final report and recommendations of the Ad Hoc Committee on 7th-Year Reviews. Our charge from the University Committee (December 11, 2017) was to "first determine whether a 7th-year review option [for probationary faculty] should exist at all" and, if so, to determine how that differs from an appeal, what the allowable conditions would be, whether such reviews should be treated as new submissions or reconsiderations, and whether reviews that happen to occur during the 7th year should even be called "7th-year reviews." Following review of practice over time in the four divisions, as well as significant deliberation and discussion, **the committee finds that, although reviews of probationary faculty do sometimes continue into the 7th year, there is no such thing as a 7th-year review per se**, nor should anything be referred to as such. Due to the confusion that surrounds reviews that continue into the 7th year (due to appeal, reconsideration, or simply time), the committee recommends clarification of language and processes to make clear that all reviews must start before the mandatory review date (ie, the end of the "6th clock year") and specify what the limitations are beyond that.

The appeals process for promotional decisions is well defined and clear, but confusion arises in the case of reconsiderations and deferrals by the divisional committee. This is particularly the case when a dossier is sent to the divisional committee late in the year. We want to be clear that submission of materials very close to the mandatory review date (end of the "6th year") should not be a method of extending an appointment or creating an additional buffer year. At the same time, we recognize that there are legitimate situations wherein a case does come up late in the probationary period, potentially causing reconsiderations or deferrals to continue into the 7th year. We also recognize that there are sometimes delays in submission that are due to circumstances beyond the control of the probationary faculty member, such as delays in requesting and receiving letters, irregular executive committee actions, or slow administrative action. Such delays and late submissions should not be viewed as prejudicial to the candidate.

For the reasons detailed above, the committee recommends clarification language in FPP to indicate that **reconsiderations must be submitted to the relevant divisional committee through the Office of the Secretary of the Faculty within 90 days of the original divisional committee decision date**. Furthermore, if a divisional committee vote is negative and the reconsideration period will extend past the mandatory review date, it should be clear that **the dean's office must issue a non-renewal letter before the mandatory review date and that the reconsideration and any eventual appeal will not extend the non-renewal date**. That is, in these situations, the affected faculty member still moves into their notice year pending the reconsideration.

Further complicating matters, the committee feels that FPP 7.07. does not appear to have been intended to allow reconsideration of divisional votes. However, each of the divisions have developed such an option for reasons of fairness and equity. The committee feels FPP is permissive on this points, so it should be clarified that it is up to the divisions to allow reconsideration if they so choose. However, **if divisional committees allow reconsideration, the rules and expectations must be clearly indicated**, providing clarity and predictability for probationary faculty, deans, and others. The committee also recommends clarification in FPP of what material should be included in a reconsideration (when allowed), again so that expectations are clear. Specifically, the committee recommends indicating that,

(continued)

except under extraordinary circumstances, completely new information will not be considered as part of a reconsideration by a divisional committee.

Another reason that reviews sometimes get delayed into the seventh year is that there is no specification in FPP of the timeframe for a dean to act on the advice of the divisional committee. Thus, **we recommend that a time limit be placed on the period between a dean receiving a recommendation from the divisional committee and the dean's action**. Specifically, FPP 7.15.F. could be changed from: "The faculty member shall be notified in writing within twenty days of the decision of the dean." to: "The faculty member shall be notified in writing within twenty days of the decision of the dean, which shall be made no later than twenty days following receipt of the divisional committee's advice."

Proposed changes:

FPP 7.06.E. Review by the departmental executive committee for the purpose of determining whether to recommend tenure must occur far enough in advance of the probationary faculty member's mandatory review date to allow for the divisional committee to also act prior to that date.

FPP 7.14.C. Each divisional executive committee shall establish written criteria and standards it will employ in recommending the granting of tenure. These criteria and standards shall assure that the granting of tenure is based on evidence of (1) teaching excellence; (2) a record of professional creativity, such as research or other accomplishments appropriate to the discipline; and (3) service to the university, to the faculty member's profession, or professional service to the public. These guidelines may include a process whereby a faculty member and/or a department or de novo review committee can request reconsideration of a decision. If such a process is allowed, the divisional guidelines must clearly specify the rules and expectations applicable thereto. It is generally expected that, except under extraordinary circumstances, completely new information will not be considered as part of any divisional committee reconsideration.

FPP 7.15.C. If the divisional executive committee advises against accepting the departmental or ad hoc committee recommendation, the departmental executive committee or ad hoc committee shall, if it so requests, be heard by the divisional executive committee and a new vote taken. Such a vote must be requested (or other documentation for reconsideration submitted to the Office of the Secretary of the Faculty) within 90 days of the original divisional committee decision date. If this 90-day period will extend past the mandatory review date, the relevant dean must issue a non-renewal letter prior to the mandatory review date and note that the reconsideration and any eventual appeal will not extend the non-renewal date.

FPP 7.15.F. The faculty member shall be notified in writing within twenty days of the decision of the dean, which shall be made no later than twenty days following receipt of the divisional committee's advice.

No mark-up

FPP 7.06.E. Review by the departmental executive committee for the purpose of determining whether to recommend tenure must occur far enough in advance of the probationary faculty member's mandatory review date to allow for the divisional committee to also act prior to that date.

FPP 7.14.C. Each divisional executive committee shall establish written criteria and standards it will employ in recommending the granting of tenure. These criteria and standards shall assure that the granting of tenure is based on evidence of (1) teaching excellence; (2) a record of professional creativity, such as research or other accomplishments appropriate to the discipline; and (3) service to the university, to the faculty member's profession, or professional service to the public. These guidelines may include a process whereby a faculty member and/or a department or de novo review committee can request reconsideration of a decision. If such a process is allowed, the divisional guidelines must clearly specify the rules and expectations applicable thereto. It is generally expected that, except under extraordinary circumstances, completely new information will not be considered as part of any divisional committee reconsideration.

FPP 7.15.C. If the divisional executive committee advises against accepting the departmental or ad hoc committee recommendation, the departmental executive committee or ad hoc committee shall, if it so requests, be heard by the divisional executive committee and a new vote taken. Such a vote must be requested (or other documentation for reconsideration submitted to the Office of the Secretary of the Faculty) within 90 days of the original divisional committee decision date. If this 90-day period will extend past the mandatory review date, the relevant dean must issue a non-renewal letter prior to the mandatory review date and note that the reconsideration and any eventual appeal will not extend the non-renewal date.

FPP 7.15.F. The faculty member shall be notified in writing within twenty days of the decision of the dean, which shall be made no later than twenty days following receipt of the divisional committee's advice.