Agenda
SENATE OF ACADEMIC STAFF MEETING
October 3, 2012
Room 217 RSSLC
3:00 p.m.

I. Call to Order
   A. Roll Call – Sign Attendance Sheet

II. Administrative Reports
   A. Chancellor's Report
   B. Vice Chancellor for Academic Affairs' Report
   C. Vice Chancellor for Administrative and Student Life Services' Report

III. Announcements

IV. Approval of Minutes of September 19, 2012 (Attachment 1)

V. Reports
   A. Chair (Jerry Addie)

VI. Old Business
   A. 2012 UW-System Academic Staff Professional Development Conference
   B. Pay Plan Update
   C. SAS Achievement Subcommittee Update
      1. Advocacy
      2. Committee Cleanup
      3. Newsletter
      4. Website
   D. University Personnel Systems
   E. Senate of Academic Staff Election Results
   F. Tobacco Free Campus Policy
   G. Other

VII. New Business
   A. Comprehensive Security Policy #10-64 (Attachment 2)
   B. SAS Achievement Subcommittees – Discussion about goals and subcommittees.
      (Attachment 3)
   C. Committee Appointments (Attachment 4)
   D. Committee Vacancies – Discussion about filling committee vacancies. (Attachment 5)
   E. ASPRO
   F. Charge to update SAS Bylaws
   G. Other

VIII. Adjournment

Notes:

1. The next Senate meeting will be held at 3:00 pm on October 17, 2012 in Oakwood Room, MSC.
Attachment 1

Minutes
SENATE OF ACADEMIC STAFF MEETING
September 19, 2012
Oakwood Room, MSC
3:00 p.m.

ATTENDANCE

CHAIR: Jerry Addie
VICE CHAIR: Krista James
PRESENT: Jerry Addie, Robert Butterfield, Nathan Castillo, James Church, Stephen Collie, Wendy Dittmann, Krista James, Josh Lind, Robin Muza, Jen Parker, Sandy White
Guests: Phil Lyons, Mary Hopkins-Best, Deb Gehrke
ABSENT: Barbara Bauer (excused), Tracy DeRusha, Susan Greene (excused), Lelah Lugo (excused), John Lui

I. Call to Order – 3:00 p.m.
   A. Roll Call – Sign Attendance Sheet
   B. SAS Executive Committee will meet immediately following the regular meeting.

II. Administrative Reports
   A. Chancellor's Report
      • Preparing for Board of Regents meeting in a couple weeks.
      • One troubling thing is that enrollment is down by 150 students (mainly continuing students). We are doing some research to find out why? Looking at the 10th day head count. It could be a larger graduating class for May 2012, versus the students who didn’t graduate, but who are not back.
      • Most important thing is the retention rate. That is a lot of revenue, accounting for approximately $300,000 in tuition. Is it showing up in specific programs or across the board?
      • Supplemental Pay Plan – We are waiting for Faculty Senate to make a determination. Once they make a decision, we can move forward. Classified staff was surveyed and they also chose “Option 3”.

   B. Vice Chancellor for Academic Affairs' Report
      • Piloting “Stout Start” for freshman - Meet as a large group once a week and then there are break-out sessions. Advisors also come to meet with groups of students. Higher risk students were told that they must participate, otherwise, it is voluntary. The goal is to help with retention.
      • Enrollment Growth Efforts – Look at opportunities for recruitment outside of Wisconsin. Currently we are down in graduate offerings, but up in CI offerings. Continue serving non-traditional students in non-traditional ways.
      • Flex Degree Meeting – is not new to UW-Stout. We are hoping to grow our certificate program options. Often people who complete their certificate program go on to complete a degree. Proposals are due 10/15/2012.
      • Racial and Ethnic Studies (RES) – There is a new requirement to be implemented in fall 2013. For A, B, and C courses, students will need 6 credits and 3 must be in A. We currently have very few A courses. The challenge is to develop A courses that also fit into another Gen Ed category. We need to add that requirement to program plan sheets. We don’t want to have hidden requirements. Gen Ed minimum: 40 Gen Ed credits.

   C. Vice Chancellor for Administrative and Student Life Services’ Report – Phil Lyons
      • Position is posted - Executive Director (reclassified from Assistant Vice Chancellor for Administrative & Student Life Services).
      • Housing has done some great things with athletics for the student athletes.

III. Announcements
IV. Approval of Minutes of September 5, 2012
Motion: James/Muza
Vote: Passed Unanimously

V. Reports
A. Chair (Jerry Addie) – See the attached link to the updates on the UPS system.
   UPS Updates
A. UPS Updates – Deb Gehrke
   1. HR plans to have UPS informational / feedback sessions in early October.
   2. Current Recommendations - Proposed Implementation Decisions
   3. Points of interest:
      a. University Staff is the new category for classified staff
      b. Move of Chapter 230 exempt/salaried employees to academic staff
         (most supervisors, IT, accounting, and technical positions)
      c. Pay all staff bi-weekly - Why would they want to pay us bi-weekly?
         Some individuals want to be paid more often and some individuals like
         the ease of budgeting. The best option would be to give people a
         choice. Right now it is not an option to allow staff to choose.
      d. Exempt classified moved into academic staff – will they get an
         unlimited appointment. A decision has not been made on this yet.
         UW-Stout is not offering indefinite appointments on campus anymore.
      e. Degree requirement for Academic Staff will be left up to individual
         campuses. There are many things left to be decided.
      f. Currently there is no talk of changing salaries.
      g. This process is not designed to eliminate people.

VI. Old Business
A. Etextbook Update – Bob Butterfield, Director of Instructional Resources
   1. Pilot Project initiated this fall using etextbooks (undergrad, grad, online, and
      face-to-face). The goal is to enhance teachers’ ability to teach and students’
      ability to learn.
   2. Opened it up to any publisher.
   3. Easier Administratively – We don’t have to worry about damaged books.
      There is no problem getting additional books or not having enough books for a
      class. There is more flexibility for instructors, if they don’t like the book, they
      can use a different book next semester.
   4. Cost Increase, Not Decrease - Because we are an established rental textbook
      college, it will definitely cost more. We don’t really have a choice because of
      publishers. Publishers are already moving to print on demand. They only print
      what they need to cut out used book dealers.
   5. Advocate for students and faculty to minimize any price increases.
   6. Definitely not a perfect system, but working to make it useable.
B. 2012 UW-System Academic Staff Professional Development Conference
C. Pay Plan Update
   1. Discussion of survey results.
      a. 151 responses out of 375 people
      b. Lots of people talking
      c. Still some confusion.
   2. Decision on how to distribute survey results.
      a. Majority of people chose #3
      b. 70% wanted a pay plan.
D. SAS Achievement Subcommittee Update
   1. Advocacy
   2. Committee Cleanup
   3. Newsletter
4. **Website**  
   **University Personnel Systems** – Discussed above.

F. **Senate of Academic Staff Election Results** – No report

G. **Tobacco Free Campus Policy** – No report

H. **Other**

VII. **New Business**

A. **SAS Achievement Subcommittees** – We will discuss this in detail at our next SAS Meeting. Do we want to continue with the same subcommittees as last year or make changes? The subcommittees are part of our strategic plan:
   - Advocacy (advocate what senate is about)
   - Committee Cleanup (committee helping to fill vacancies)
   - Newsletter (complete a newsletter once every 6 weeks - new member needed)
   - Website (keep website current)

Committee Membership needs to be looked at again. Every committee has a charge and something in writing. We need to update what we plan to do.

B. **Committee Appointments**

   **Motion:** Collie/Muza
   **Vote:** Passed Unanimously

C. **Committee Vacancies** – How to proceed in filling these vacancies? This will be discussed at the next meeting.

D. **Other**

VIII. **Adjournment** 4:38 p.m.

**Notes:**

1. *The next Senate meeting will be held at 3:00 pm on October 3, 2012 in Room 217 RSSLC.*

Recorded and prepared by,  
Brenda Krueger
TO:  Jerry Addie  
    Ned Weckmueller  
    c: Meridith Drzakowski  
    Kristi Krimpelbein  
    Brenda Krueger  
    Doug Wahl  

via electronic mail

FROM:  Charles W. Sorensen  
    Chancellor  

DATE:  September 25, 2012  

RE:  Comprehensive Security Policy: #10-64

This memo is to request a formal review and resolution by the Faculty Senate and the Senate of Academic Staff of a new policy entitled Comprehensive Security Policy: #12-70. Your resolution would be appreciated by October 12, 2012. The policy was developed by the Policy Review Committee that included Len Pederson and Krista James as faculty and academic staff representatives. The policy has been reviewed by the campus policy committee and the Chancellor’s Cabinet.

The policy serves as a guide to ensure that computing resources are used ethically and responsibly within the university community. Doug Wahl can serve as a resource person for any questions.

Thank you for your consideration of this new policy.

Attachment
University of Wisconsin-Stout Policy
COMPREHENSIVE SECURITY POLICY

Policy No. 10-64
Date: 09/11/2012

1.0 INTRODUCTION

The University of Wisconsin – Stout (UW-Stout) supports freedom of expression and an open environment for scholarly research. The contents of the UW-Stout computer systems must comply with university policy, as well as local, state, and federal laws. This document is not meant to be a comprehensive list of what is allowed and not allowed, but a guide to ensure that computing resources are used ethically and responsibly within the university community. Effective security involves the participation and support of every university employee and student and computer user. It is the responsibility of every computer user to familiarize themselves with these guidelines and to conduct activities accordingly.

2.0 STATEMENT OF POLICY

This policy applies to all users of UW-Stout information technology resources, irrespective of whether those resources or data are stored on or accessed from on-campus or off-campus locations. Unauthorized users are not protected by this policy.

The purpose of this policy as a whole is:

- To protect and ensure the integrity of student and employee information
- To follow applicable state and federal laws related to copyright and data security
- To develop procedures to ensure the physical security and appropriate access of data
- To ensure adherence to software compliance and usage guidelines
- To outline procedures for the secure use of email and other internet activities
- To provide guidelines for ensuring greater security between UW-Stout and all users with access to UW-Stout systems and information
- To prevent copyright infringement
- To protect the integrity of the UW-Stout computer environment

3.0 GUIDELINES FOR IMPLEMENTATION

3.1 Storage of Copyrighted Material on UW-Stout Systems

UW-Stout retains all ownership of its computer and network systems. Copyrighted material that is not legally licensed should not be stored on UW-Stout owned systems in accordance with the Digital Millennium Copyright Act.

3.2 Information Handling

In order to uphold strong privacy and security expectations, the university will ensure compliance with FERPA and HIPAA regulations regarding the exchange, storage, and retrieval of protected electronic information.

3.2.1 Care and Handling of Internal Information
Data custodians will be trained in the type of information that can be disclosed to others. It is the responsibility of the custodian to verify that the information requested will be used in accordance with state, federal and university policies.

3.2.3 Data Misuse

*See University Policy 09-66*

Individuals are not allowed to retain copies of any non-public files after ending employment at UW-Stout. Non-public files include, but are not limited to, documents accessible only through the intranet, Qualtrics surveys, and internal job-related documents housed on a department’s shared drive or an individual’s personal drive, unless they are also available on the internet. Exceptions include instructional materials developed by the instructor (see Intellectual Property Administrative Procedure and the UW-Stout Faculty handbook section on copyrighting instructional materials for more details).

3.3 Access

3.3.1 Employee Username and Password Responsibilities:

The Chief information Officer (CIO) or designee is responsible for the development of guidelines that ensure passwords are secure and confidential.

Password Complexity Requirements: see appendix A

3.3.2 Access to Personal Identifiable Information (PII)

Anyone who has access to another’s PII as defined by Wisconsin Statute 134.98 must conform to Level of Assurance (LOA) 2 requirements: see appendix B.

3.3.3 Human Resources responsibilities

The Human Resources Office is responsible for notifying Learning and Information Technology (LIT) when (or before) an employee leaves the university or transfers to another department so that access can be revoked.

3.3.4 Guest and Special Access

Granting access to network resources to individuals other than employees of the university may be necessary on occasion. If access is needed by external individuals, it should be requested from LIT. Examples of such individuals are consultants, review board members, and volunteers. Employees must never give out their passwords to others.

LIT reserves the right to refuse access to any such individual if access is in violation of information security guidelines for acceptable use or in violation of any applicable laws.

3.3.5 Access Audits

LIT may routinely audit access to university computing resources and reserves the right to temporarily disable questionable access. Department heads are responsible for periodically reviewing access to their information and must notify LIT if access should be revoked or levels changed.
3.4 Software Guidelines

3.4.1 Purpose

It is the intent of the UW-Stout to respect all computer software copyrights and adhere to the terms of all software licenses to which UW-Stout is a party. The university shall take all steps necessary to prohibit users from duplicating any licensed software or related documentation for use either on UW-Stout premises or elsewhere, unless expressly authorized to do so by the licensor. Unauthorized duplication of software may subject users and the University to both civil and criminal penalties under the United States Copyright Act, 17.

In accordance with US copyright laws, UW-Stout must not permit any employee to use software in any manner inconsistent with the applicable license agreement or terms of use when the software is received as part of a grant, gift or donation. This includes giving or receiving software or fonts from students, colleagues, or others.

3.4.2: Software Compliance

UW-Stout licenses the use of computer software from a variety of outside companies. The university does not own this software or its related documentation. Unless expressly authorized to do so, the university has no right to make copies of the software except for backup or archival purposes.

LIT will only install client applications as expressly permitted by its associated license agreement.

3.4.4 Penalties and Reprimands

Any UW-Stout computer user, who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances, according to the US Copyright Act. Such discipline may include termination of employment or suspension from the university.

3.5 Mobile Computing

3.5.1 Purpose

This applies to any mobile computing device connected to UW-Stout Information Technology resources, used to process or store university data, or conduct university business. Mobile devices include various types of equipment such as PDAs, smartphones, tablets or netbook computers.

Mobile Device Guidelines: see appendix C

3.5.2 Security Provisions

It is the responsibility of the user to ensure that information stored on the mobile device is protected as required by applicable state and federal laws such as FERPA and HIPAA. Users must meet the security provisions detailed in the Mobile Device Guidelines before the device is used to process or store university data or connect to UW-Stout information technology resources.

Users must be aware that all information synced from the UW-Stout network is the property of the university and not the individual.
Personal Digital Assistants (PDAs), tablets and smartphones are not considered secure computing devices. Under no circumstances should confidential and sensitive information be stored on a device of these types.

3.6 Security Incident Reporting: LIT should be notified immediately with any security incident reporting. See appendix D for more information

4.0 DEFINITIONS

4.1 Authorized User:

A university employee, student, or other individual affiliated with the university who has been granted authorization to use a specific electronic resource.

4.2 Backup:

To create a copy of critical files to minimize the loss of data in the event of a system failure.

4.3 Chain or email letter: Email sent to successive people.

Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

4.4 Date Custodian:

Responsible for the safe custody, transport, storage of data and the implementation of business rules.

4.5 Data Misuse:

Using university-owned data (either unintentionally or intentionally) in a manner inconsistent with university policy, or federal, state, or local laws.

4.6 Digital Millennium Copyright Act (DMCA):

Unauthorized production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works. It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself.

4.7 Electronic Resource:

Material in digital format which requires a computer device for use.

4.8 Email:

All electronic mail communications and associated attachments transmitted or received.

4.9 Employee:

A person hired by the University of Wisconsin-Stout, whose primary role is to work for wages and salary.

4.10 Encryption:

A security method used to transform data from its original form into a difficult to interpret format in order to prevent any but the intended recipient from reading that data.
4.11 External information:

Information collected, bought, or given by a source outside the university. Often, this information comes with copyright or confidentiality agreements that dictate how the information is used. The university will adhere to any such agreements accompanying this information.

4.12 Extranet:

Private network that uses internet protocols to securely share part of an organization’s information or operations with suppliers, vendors, partners, customers or other businesses.

4.13 Family Educational Rights and Privacy Act (FERPA):

A federal law enacted in 1974 protecting the privacy of student education records (see USC 20, 123g for a complete definition).

4.14 Fair Use:

The use of portions of copyrighted material for the purpose of commentary and/or criticism.

4.15 Firewall:

An access control device that acts as a barrier between two or more segments of a computer network used to protect internal networks from unauthorized users or processes of other networks.

4.16 Firmware:

Computer program that is embedded in a hardware device.

4.17 Forwarded email:

Email resent from an internal network to an outside point.

4.18 Health Insurance Portability and Accountability Act of 1996 (HIPAA):

An act authorizing the development of security and privacy standards to protect healthcare information that is stored electronically.

4.19 Host:

A computer connected to the network.

4.20 Intellectual Property:

Ownership of ideas and control over the tangible or virtual representation of those ideas.

4.21 Internal Information:

Information collected and maintained by the University. UW-Stout is the owner of this information.

4.22 Internet:
A global system of interconnected computers and computer networks. The computers and networks are owned and maintained separately by a host of organizations, government agencies, companies, and colleges and exist outside the UW-Stout network.

4.23 Intranet:

Private network that uses internet protocols to securely share part of an organization’s information or operations with its employees.

4.24 Institutional Purposes:

Broadly defined as legitimate items directly related to the mission of the university.

4.25 Learning and Information Technology (LIT):

The university department responsible for the purchasing recommendations, management, and support of computer, network, and telecommunications systems on campus.

4.26 Level of Assurance (LOA):

The degree of confidence in identity assurance.

4.27 Logon:

See “Username”

4.28 Mobile Computing:

The ability to use technology in a non-fixed or non-static environment or location, via a portable computing or communication device such as a laptop, tablet, PDA, or cell phone.

4.29 Password:

A string of characters known only to the user that serves as authentication of a person’s identity. Passwords may be used to grant, or deny, access to information or resources. Access to systems or information is usually granted by a combination of username and password.

4.30 PDA:

Personal Digital Assistant (PDA) is a handheld computer used as mobile phones, web browsers, or portable media players.

4.31 Personal Identifiable Information (PII):

Information related to a person’s private life or concerns, recorded in any form, by which individuals can be identified. Personal information can include: name, address, telephone number, race, ethnic origin, Driver’s License or State Identification number, bank account numbers, or social security numbers.

4.32 Personal Files:

Any type of record, document, or file that is of a personal nature and does not relate to the university or university business.

4.33 Privileged Information:
Information confined to an exclusive or chosen group of users. Privileged information is not considered common knowledge, or has not been cleared for release to others outside the group.

4.34 Public Records:

All writings made, maintained, or kept by the university for use in the exercise of functions.

4.35 Reasonable Efforts:

Efforts based on known statements, events, or conditions. Reasonable efforts are defined as being within common sense, known best practices, or logical actions.

4.36 Remote Access:

The ability to obtain access to an IT resource or the UW-Stout networks from a location other than the physical campus of the University of Wisconsin - Stout, located in Menomonie, WI, or via a system or device not owned by the University of Wisconsin – Stout.

4.37 Security:

Measures taken as to ensure a reliable computing platform free from the risk of loss.

4.38 Security incident:

An act that violates an explicit security policy. Violations may include events having actual or potential adverse effects which compromise an aspect of computer, network or user resources, including but not limited to: loss of confidentiality of information; a compromise of the integrity of information; misuse of service, systems of information; damage to systems or loss of property or information

4.39 Sensitive Information:

Information is considered sensitive if it can be damaging to UW-Stout or its customers reputation or market standing.

4.40 Server:

A system or computer program that provides information or services to other programs or devices.

4.41 Spam:

Unauthorized and/or unsolicited electronic mass mailings.

4.42 Student:

Person who is enrolled for study, as their primary role, at the University of Wisconsin - Stout.

4.43 Tablet:

Portable personal computer equipped with a touchscreen as a primary input device.

4.44 TCP/IP:
Transmission control protocol/internet protocol. This is a combined set of communication protocols that are used to perform data transfers between computers. These protocols are used to communicate over the internet.

4.45 Unauthorized Disclosure:

The intentional or unintentional revealing of restricted information to people, both inside and outside UW-Stout, who do not have a need to know that information.

4.46 User:

Any individual who uses, logs in, attempt to use, or attempts to log into a system, whether by direct connection (modem or network) or across one or more networks.

4.47 UserID:

see “Username”

4.48 Username:

Also referred to as “logon” or “userID”. A unique string of characters used to identify a specific user in a multi-user environment. Access to systems or information is usually granted by a combination of Username and Password.

4.49 Virtual Private Network (VPN):

A private data network established within or across a public network that utilizes various security methods to transfer information.

4.50 Virus Warning:

Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

4.51 Wireless Network:

A network utilizing radio waves to transmit data as opposed to physical wired connections. Common terms used to describe a wireless network include Wi-Fi, WLAN, or 802.11.

4.52 Webmaster:

Person responsible for designing, managing, maintaining, and updating the website and web server.

5.0 REFERENCES

Copyright Law U.S. Code Title 17

Digital Millennium Copyright Act (DMCA) 17 USC 101

Family and Educational Rights and Privacy Act (FERPA) 34 CFR 99

Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191)

State of Wisconsin Statute 134.98
Appendix A

Password Requirements

A network password is the key to access most systems on campus. All UW-Stout employees and users are expected to keep ALL system passwords private. All passwords will conform to LOA requirements based on the users level of data access.

In addition, we strongly recommend:

- Never use a person’s name or any word that could be found in the dictionary. Breaking up words with special characters or numbers is an easy way to avoid this.
- Do not use the same passwords for work as you do for personal use

If a password is entered incorrectly twenty times in a row, the account will be locked and the user will not be able to log on until the lockout expires.

If a password is forgotten or needs to be reset, the user will be required to go to the password page on the campus website to resolve the issue. Passwords will not be sent via mail or email, or given to others.
Appendix B

Level of Assurance (LOA) Password Security Requirements

Passwords must meet the following requirements for all levels

- It must not contain all or part of the user's account name
- It must contain characters from at least three of the following four categories:
  1. English Uppercase characters (A through Z)
  2. English Lowercase characters (a through z)
  3. At least one number (0-9)
  4. Non-alphanumeric characters (example: $, #, %, ^)

LOA1 additional security measures include:

- Password must have a minimum of eight (8) characters
- 30 minute lockout after 20 login failed attempts applies to all levels
- Change of password every 365 days

LOA2 additional security measures include:

- Password must have a minimum of fifteen (15) characters
- Change of password every 90 days
- Idle system lockout after 10 minutes

LOA3 additional security measures include:

- Password must have a minimum of fifteen (15) characters
- Change of password every 45 days
- Idle system lockout after 5 minutes
Appendix C

Mobile Device Guidelines

UW-Stout employees are using mobile devices (cell phone, iPad, tablets, etc.) and their related technology increasingly as a means of sending and receiving UW-Stout email, synchronizing calendars and contacts, transmitting text messages and connecting to the internet. The purpose of this guideline is to:

1. Assist employees who purchase mobile devices and plans independent of UW-Stout with connecting to our servers for email and other online services;
2. Describe how UW-Stout manages mobile device technology to minimize risk, especially in the event of loss or theft;
3. Remind employees about the appropriate use of email by offering helpful hints

UW-Stout recognizes that some employees, although not required to carry a cell phone as part of their position responsibilities, would still like to connect their own device to UW-Stout’s Active Sync Server so they can access and synchronize their email, contacts and calendar. Employees interested in connecting to our Active Sync Service should visit the ASK5000 knowledgebase for the necessary server information. Given the vast number of mobile devices on the market, ASK5000 will provide ‘best effort’ support. Connectivity cannot be guaranteed. Users are encouraged to contact their provider for in-depth support.

The nature of mobile devices such as tablets and cell phones lends to a greater risk of loss. The fact that mobile devices can also be used to store information like email, contacts and documents serves to increase the risks associated with such loss, but there are software policies that can be placed on the device to help minimize this risk.

If an employee, either because of work-related requirements or through their own choosing, elects to access UW-Stout email and documents via their mobile device, they must do so by:

- connecting to UW-Stout’s Active Sync Server, and
- accepting the security policies downloaded onto the device as a result of that connection

Please note these security policies are designed to accomplish three primary objectives:

1. Require a password to access the information on the device;
2. Automatically wipe the data on the device in the event of ten failed login attempts;
3. Enable the user or Telecommunications and Networking Administrators at the users request, to remotely wipe the UW-Stout email and calendar data in the event that the device is lost or stolen.
Appendix D

Security Incident Reporting

Learning and Information Technology should immediately be notified with the following information:

- Date and time of incident
- Type of incident and any other pertinent details that would assist in verifying incident
- A statement describing the impact on users, department or the network including the number of users/departments affected.
- Contact information of submitter

Return to Sequential Index.
Return to Subject Index.
### Action Plan:

#### Goals

**Website** – To develop a more informative Senate of Academic Staff website and to capitalize on the opportunity to improve web presence with the new website format.

**Newsletter** – Develop an electronic newsletter to share Senate information with all Academic Staff.

<table>
<thead>
<tr>
<th>Action Plan:</th>
<th>Task:</th>
<th>Responsible:</th>
<th>Timeline:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Website</strong> – To develop a more informative Senate of Academic Staff website and to capitalize on the opportunity to improve web presence with the new website format.</td>
<td>“What action item will you implement to support this plan?”</td>
<td>Josh Lind, John Lui, Jen Parker</td>
<td>June 1, 2012</td>
</tr>
<tr>
<td></td>
<td>Update all current information and identify areas for new content</td>
<td>Josh Lind, John Lui, Jen Parker</td>
<td>August 31, 2012</td>
</tr>
<tr>
<td></td>
<td>New content to include: comment/suggestion link, contact your SAS Rep, what’s new?</td>
<td>Josh Lind, John Lui, Jen Parker</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add instructions on how to utilize Image Now to retrieve previous agendas, minutes, resolutions, etc</td>
<td>Josh Lind, John Lui, Jen Parker</td>
<td>June 1, 2012</td>
</tr>
<tr>
<td></td>
<td>Use google analytics to measure web traffic and determine whether or not traffic increases as a result of increased SAS exposure</td>
<td>Josh Lind, John Lui, Jen Parker</td>
<td>Begin March 1st - ongoing</td>
</tr>
<tr>
<td><strong>Newsletter</strong> – Develop an electronic newsletter to share Senate information with all Academic Staff</td>
<td>Determine frequency of the newsletter. Goal is to publish 3 each semester.</td>
<td>Barb Bauer, Paul Roberts, Krista James, Tim Mertz</td>
<td>Begin October 2011 - ongoing</td>
</tr>
<tr>
<td></td>
<td>Determine the content of the newsletter and solicit contributions from other Senators:</td>
<td>Barb Bauer, Paul Roberts, Krista James, Tim Mertz</td>
<td>Begin October 2011 - ongoing</td>
</tr>
<tr>
<td></td>
<td>Develop format and incorporate Integrated Marketing Identity Standards.</td>
<td>Barb Bauer, Paul Roberts, Krista James, Tim Mertz</td>
<td>February 2012</td>
</tr>
</tbody>
</table>
## Committee Cleanup

- **Work with the PARQ office and the Faculty Senate to implement a process to better advertise committees and fill vacancies**
  
  - Review and revise the Election Process for Committees document. Seek input from the PARQ office, the Faculty Senate and Janell
  - Work with the Faculty Senate to create a procedure for advertising committee openings – develop timeline
  - Promote all Academic Staff Committees and have them added to the committee list document
  - Utilize the SAS website to promote committee involvement

<table>
<thead>
<tr>
<th>Task</th>
<th>Responsible Parties</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review and revise the Election Process for Committees document</td>
<td>Wendy Dittmann, Susan Greene, Jen Rudiger</td>
<td>March 1, 2012</td>
</tr>
<tr>
<td>Work with the Faculty Senate to create a procedure for advertising committee openings – develop timeline</td>
<td>Wendy Dittmann, Susan Greene, Jen Rudiger</td>
<td>April 1, 2012</td>
</tr>
<tr>
<td>Promote all Academic Staff Committees and have them added to the committee list document</td>
<td>Wendy Dittmann, Susan Greene, Jen Rudiger</td>
<td>March 1, 2012</td>
</tr>
<tr>
<td>Utilize the SAS website to promote committee involvement</td>
<td>Wendy Dittmann, Susan Greene, Jen Rudiger</td>
<td>April 1, 2012</td>
</tr>
</tbody>
</table>

## Advocacy

- **Serve as advocates for Academic Staff during the UW System Restructuring and Facilities Operational Review.**
  
  - Review and advocate for the preservation or improvement of current contract options
  - Increase the participation of Academic Staff at campus listening and engagement sessions – work with PARQ office to track Academic Staff attendance.
  - Advocate and assist with marketing efforts for the annual Chancellor's Award for Academic Excellence.

<table>
<thead>
<tr>
<th>Task</th>
<th>Responsible Parties</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review and advocate for the preservation or improvement of current contract options</td>
<td>Matt Bessen, Amy Gullixson, Amy Nord</td>
<td>Begin October 2011 - ongoing</td>
</tr>
<tr>
<td>Increase the participation of Academic Staff at campus listening and engagement sessions – work with PARQ office to track Academic Staff attendance.</td>
<td>Matt Bessen, Amy Gullixson, Amy Nord</td>
<td>Begin February 2012 - On going</td>
</tr>
<tr>
<td>Advocate and assist with marketing efforts for the annual Chancellor's Award for Academic Excellence.</td>
<td>Matt Bessen, Amy Gullixson, Amy Nord</td>
<td>February 8th, 2012</td>
</tr>
</tbody>
</table>
### Attachment 4

**SAS Committee Appointments**

10/03/2012

<table>
<thead>
<tr>
<th>Committee</th>
<th>Academic Staff Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive Action, Ethics and Competition Review Committee – CSTEM</td>
<td>Jim Church</td>
</tr>
<tr>
<td>Positive Action, Ethics and Competition Review Committee – CSTEM</td>
<td>Dennis Schmidt</td>
</tr>
<tr>
<td>Committee Name</td>
<td># of Vacancies</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Faculty and Academic Staff Professional Development Grants Review Committee</td>
<td></td>
</tr>
<tr>
<td>Positive Action, Ethics, and Competition Review Committee</td>
<td></td>
</tr>
<tr>
<td>3 openings in ASA (1 @ 2 year &amp; 2 @ 1 year)</td>
<td>-</td>
</tr>
<tr>
<td>Positive Action, Ethics, and Competition Review Committee</td>
<td></td>
</tr>
<tr>
<td>2 openings is ASLS (2 @ 2 year)</td>
<td>-</td>
</tr>
<tr>
<td>Positive Action, Ethics, and Competition Review Committee</td>
<td></td>
</tr>
<tr>
<td>1 opening in Chancellor’s Division (1@1year)</td>
<td>-</td>
</tr>
<tr>
<td>Positive Action, Ethics, and Competition Review Committee</td>
<td></td>
</tr>
<tr>
<td>2 openings in CAHSS</td>
<td>-</td>
</tr>
<tr>
<td>Positive Action, Ethics, and Competition Review Committee</td>
<td></td>
</tr>
<tr>
<td>2 openings in CEHHS</td>
<td>-</td>
</tr>
<tr>
<td>Positive Action, Ethics, and Competition Review Committee</td>
<td></td>
</tr>
<tr>
<td>1 opening in COM</td>
<td>-</td>
</tr>
<tr>
<td>TOTAL VACancies</td>
<td>11</td>
</tr>
</tbody>
</table>