Ohio University Administrative Senate
Minutes of May 21, 2015
HRTC, Room 154

Next Meeting: June 18, 2015
12:10 p.m. – 1:30 p.m.
Baker Center, Room 240

Present: Jewell Barlow, Martin Barnes (online), Nicholas Brigatti, Lisa Dael, Marissa Dienstag, Tim Epley, Doug Grammer (online), Christina Jenkins, Laurie Lach (online), Feliz Levy (online), Jennifer Maskiell, Marjorie Mora (online), Kelly Pero, Connie Pollard, Corey Posey (online), Wendy Rogers, Andrew Stuart, Eileen Theodore-Shusta, Cathleen Waller, Matt Ward, Jessica Wingett, Eleni Zulia

Excused: Joshua Bodnar, Misti Smith

Absent: Myca Haynes, Toni Heightland, Ricky Huard, Wendy Kaaz, Melissa Standley

Guests: Matthew Dalton, Sarah Lack (online), Joseph Lalley, Deborah Shaffer, Duane Starkey

Call to Order: Cathleen Waller called the meeting to order at 12:10 p.m.

Approval of Minutes: Cathleen Waller asked for a motion to approve the minutes of the April 16, 2015 meeting; Kelly Pero moved, Eileen Theodore-Shusta seconded the motion, a vote was taken, and the minutes were unanimously accepted.

Chairperson’s Report: Cathleen Waller reported that the Benefits Advisory Council is looking at possibly offering a higher deductible healthcare option.

Vice Chairperson’s Report: No Report

Secretary’s Report: No Report

Treasurer’s Report: The April 2015 Budget Report is attached. Charges are still coming in for the Administrative Service Awards and all charges will be closed by the end of this fiscal year.

Committee Reports: After a few glitches with the election process, over 150 administrators voted this year vs. 100 voters last year. Yesterday, Jessica Wingett sent an email to Human Resources for status verification on each voter. The results are expected back in the next week or so. Once the results are back, Wingett will forward them to Cathleen Waller, who will then send out an announcement.

Jewell Barlow reported that the Tobacco Free webpages are in place. The committee is in the process of getting the word out and periodic litter cleanups will be scheduled. A map will be created to identify boundaries, and smoking is permitted on city property. It is each manager’s responsibility to enforce the policy. According to the 2344 responses from the Qualtrics Survey, 436 (19%) staff say they smoke or use tobacco products on campus. There is a blanket statement recommended to use on all communication. Outside vendors and independent contractors will be informed of the policy.
Old Business: Senate will move forward with redistricting as departments have shifted and some buildings are no longer occupied. Contact Cathleen Waller, Waller@ohio.edu if interested in working with the Executive Committee or have suggestions.

New Business: None

University Update – Duane Starkey, Interim Chief Information Officer and Director of Systems & Operations, and Matthew Dalton, Director of Information Security, Office of Information Technology: Matthew Dalton presented on the Password Policy review. About 18 months ago there was an increase in compromised accounts. An audit was launched and a tool was used that allowed the University to assess the strength of passwords. The tool ran for one (1) hour and 15% of all passwords were predicted. An audit is done annually by the audit firm Plante Moran and for the past 4 – 5 years, one of their recommendations has been to increase the strength and length of passwords used. Peer institutions and IUC schools were looked at. The rollout will be over 15 months and an email will be sent giving users the opportunity to change their password when it is convenient for them. Passwords will expire if they are not changed at the end of 15 months. All University systems will use this policy, and includes devices. Dalton asked the Senators to review and provide feedback; his email is Daltonm@ohio.edu. A copy of the DRAFT policy and Authentication Credentials Complexity Standard are attached.

University Update – Joseph Lalley, Senior Associate Vice President for Information Technology & Administrative Services: Joseph Lalley stated that the steam that was turned off to Campus last week due to needed repairs will be turned back on May 26 to most buildings on campus. The exceptions are McCracken, Siegfried, College of Fine Arts, and Patton College of Education due to additional repairs. Hot water will be turned on for Wellness and the Aquatic Center May 29.

University Update – Deborah Shaffer, Senior Associate Vice President for Finance & Administration: Deborah Shaffer informed Senate that Partner Groups are being formed and an announcement on what groups are formed and how to contact co-chairs if interested in participating is forthcoming. The groups will be structured on a 2-year cycle and will be staggered to allow for more participation.
● The University is moving forward with the reappointment process, but a decision on raises, including the Faculty Comp Plan, and Comp 2014, is delayed until more information is received on the State budget process. The decision will be made later this summer and will be retroactive to July 1. There is still talk about a rollback which may affect the tuition Guarantee and auxiliary operations.

Discussion and Announcements: The names of this year’s Outstanding Administrators are being added to the Outstanding Administrators board outside of Chubb Hall.

Adjournment: Cathleen Waller asked for a motion that the meeting be adjourned, Eleni Zulia moved, Lisa Dael seconded, the motion passed unanimously, and the meeting adjourned at 1:00 p.m.

Respectfully submitted,

Wendy Rogers
Secretary

Debbie Crabtree
Assistant to the Senate

Next Meeting: June 18, 2015
12:10 p.m. – 1:30 p.m.
Baker Center, Room 240
<table>
<thead>
<tr>
<th>Admin Senate</th>
<th>Period Activity</th>
<th>Budget</th>
<th>Funds Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>APR 2015-15</td>
<td>$ 5,712.93</td>
<td>$ 30,168.00</td>
<td>$ 45,330.70</td>
</tr>
<tr>
<td>100000's - Professional Srvcs &amp; Misc</td>
<td>$ -</td>
<td>$ -</td>
<td>$ (160.00)</td>
</tr>
<tr>
<td>300000's - Supplies</td>
<td>$ -</td>
<td>$ -</td>
<td>$ (1,155.71)</td>
</tr>
<tr>
<td>400000's - Travel &amp; Entertainment</td>
<td>$ -</td>
<td>$ 14,682.00</td>
<td>$ 14,536.00</td>
</tr>
<tr>
<td>500000's - Communication</td>
<td>$ 1,097.31</td>
<td>$ -</td>
<td>$ (6,397.04)</td>
</tr>
<tr>
<td>600000's - Maintenance Operations</td>
<td>$ 300.00</td>
<td>$ -</td>
<td>$ (320.00)</td>
</tr>
<tr>
<td>700000's - Miscellaneous</td>
<td>$ 209.70</td>
<td>$ -</td>
<td>$ (564.88)</td>
</tr>
<tr>
<td>Administrative Salaries</td>
<td>$ -</td>
<td>$ 13,327.00</td>
<td>$ 13,327.00</td>
</tr>
<tr>
<td>Benefits</td>
<td>$ 201.16</td>
<td>$ 2,159.00</td>
<td>$ 625.77</td>
</tr>
<tr>
<td>Classified Wages</td>
<td>$ (124.54)</td>
<td>$ -</td>
<td>$ (915.17)</td>
</tr>
<tr>
<td>Faculty Salaries</td>
<td>$ 1,029.30</td>
<td>$ -</td>
<td>$ (8,721.27)</td>
</tr>
<tr>
<td>Healthcare</td>
<td>$ -</td>
<td>$ -</td>
<td>-</td>
</tr>
<tr>
<td>Inter (Across) Unit Allocations</td>
<td>$ -</td>
<td>$ -</td>
<td>$ (350.00)</td>
</tr>
<tr>
<td>Non-Mandatory Transfers to (from) Operations Funds</td>
<td>$ -</td>
<td>$ -</td>
<td>$ 38,426.00</td>
</tr>
<tr>
<td>Other Payroll</td>
<td>$ 3,000.00</td>
<td>$ -</td>
<td>$ (3,000.00)</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td>$ 5,712.93</td>
<td>$ 30,168.00</td>
<td>$ 45,330.70</td>
</tr>
</tbody>
</table>
### Status:
Draft Version 2 of March 16, 2015

### Signatures and dates on archival copy

#### Effective:
[“when approved,” or “30 days after approval,” or a specific future date]

#### Initiated by:
Matthew Dalton  
Director, Information Security

#### Endorsed by:
Pam Benoit  
Executive Vice President and Provost

#### Approved by:
Roderick J. McDavis  
President

---

**Editorial Note:** The policy main body text is organized in outline format: sections by Roman Numerals starting with I, subsections by capital letters starting with A, Arabic-numbered lists starting with 1. Sections and subsections have “captions” or “headings” on the same line with the Roman numeral or the capital letter. Itemized lists in sections that have no subsections use capital letters, starting with A. For detailed specifications, see:

[http://www.ohio.edu/policy/01-001.html](http://www.ohio.edu/policy/01-001.html)

[http://www.ohio.edu/policy/guidelines.html](http://www.ohio.edu/policy/guidelines.html)

[http://www.ohio.edu/policy2/resources.html](http://www.ohio.edu/policy2/resources.html)

[http://www.ohio.edu/policy2/trackchanges.html](http://www.ohio.edu/policy2/trackchanges.html)
You need not worry about the left margins and font sizes while working with your Word draft, those will be adjusted in the HTML version.

I. Overview
Credentials issued at Ohio University are for the sole purpose of accessing university resources. They are often the first line of attack, and the last line of defense, in the protection of these resources. Because of this, they must be used with care, and adequately protected. This policy outlines those protections that must be observed by individuals, technical staff, and systems using credentials at the university and recommendations for their protection.

II. Individuals
An individual to whom credentials have been issued has certain responsibilities in the care of those credentials. The following behaviors should be observed to reduce the risk of compromise to your credentials.

1. Keep your credentials, secret questions, and their answers private and known only to you.
2. Use unique credentials (username/password combination) for Ohio University that are different from any other service or website.
3. Your credentials are for your personal authentication to university resources, and should not be used as a means to provision services to other users.
4. If you suspect that your credentials have been compromised, change your credentials and questions immediately and inform the Information Security Office at security@ohio.edu.

III. Credentials
Credentials exist to ensure that the individual gaining access to university resources through an account is the same individual to whom the access was given. The university acknowledges that not all accounts carry the same level of risk. Therefore the level of rigor and complexity requirements that are applied to ensuring the security of the credentials will be in line with the risk which a compromise of that account would present to the university or its community.

The University Data Stewards will review these complexity requirements on an annual basis. Any changes that need to take place between reviews will be identified by the University Information Security Officer, and presented to the University Data Stewards for approval. Actual authentication complexity requirements will be captured in the
Authentication Credentials Complexity Standard, which strives to relate the strength of the credential with the risk that a compromise of that account would present to the University.

IV. Information System Owners
It is the owner or manager of information services’ responsibility to ensure that they comply with this policy and its associated complexity requirements. The recommended method is integrating with OIT authentication services and appropriately mapping individuals’ accounts to the correct risk levels. Prior to integrating with OIT authentication services, permission must be obtained from the University Information Security Officer and the Chief Information Officer or their delegates. If a separate user credential is issued, the service owner must instruct their users to use different credentials than their OhioID.

V. Authentication Servers
University Authentication Services are limited to those run and maintained by the Office of Information Technology. It is the responsibility of the Chief Information Officer or appointed delegate to ensure that the following are adhered to by all systems that perform authentication functions.

1. Only those systems that are required and approved by the Chief Information officer or appointed delegate may store passwords in any form. Those that store these passwords must store them in a cryptographically secure format.
2. Authentication systems must encrypt password at all times during transmission.
3. Authentication systems must be housed in the University Datacenter or an approved location.
4. Authentication systems must be administered by OIT.
5. Authentication systems must be hardened in accordance with NIST 800-123.
6. Administrators accessing authentication systems must use an approved multi-factor authentication to access.

Reviewers

Proposed revisions of this policy should be reviewed by:

A. [list reviewers]

[Editorial Note: do not list the people in the signature block, nor those people or committees that review all policies, through their roles in the review and approval process, as specified in Policy 01.001; do list all those people who have roles specified by this policy, even if they are among those who review all policies or are in the signature block.]
Forms, References, and History

A. Forms

The following forms are specific to this policy:

1. [list each form by name, with linked URL or other method to obtain]

B. References

The following items are relevant to this policy:

1. [list each item, with linked URL or other method to obtain]

C. History

Draft versions of this policy that were circulated for review, their cover memos, their forms, and Reviewers’ comments on them are available on the password-protected Review site, at https://www.ohio.edu/policy2/00-000/.

There are no prior versions of this policy.

(or)

Prior versions of this policy were approved on [list of dates in reverse chronological order; if three or more, as a bulleted list]

[Editorial Notes: Change the “00-000” in the first paragraph to match the number of this policy, but still with a hyphen not a period between the parts.

You need not worry about the dates of the prior versions, those will be added by OIT staff, based on the archives, when the HTML version is prepared. You are welcome to list the dates you do know about, to ensure that we don’t miss them.]
Authentication Credentials Complexity Standard

Table of Contents

Revisions .................................................................................................................................................. 2
Overview ................................................................................................................................................. 3
Risk Levels ............................................................................................................................................ 3
   Risk Level 1 .................................................................................................................................... 3
   Risk Level 2 .................................................................................................................................... 3
   Risk Level 3 .................................................................................................................................... 3
   Risk Level 4 .................................................................................................................................... 3
Standards for Credentials at Ohio University ......................................................................................... 4
   Character Classes ............................................................................................................................ 4
   Dictionary Words .............................................................................................................................. 4
   Length ............................................................................................................................................... 4
   Expiration ......................................................................................................................................... 4
   Password Reuse ............................................................................................................................... 4
Credential Level 1 .................................................................................................................................. 4
Credential Level 2 .................................................................................................................................. 4
Credential Level 3 .................................................................................................................................. 4
Credential Level 4 .................................................................................................................................. 5
<table>
<thead>
<tr>
<th>Author</th>
<th>Date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matthew Dalton</td>
<td>10/21/14</td>
<td>Initial Creation</td>
</tr>
<tr>
<td>Matthew Dalton</td>
<td>1/13/15</td>
<td>Revisions from Comments</td>
</tr>
<tr>
<td>Matthew Dalton</td>
<td>1/27/15</td>
<td>Revisions from Comments by Data Stewards</td>
</tr>
</tbody>
</table>
Overview
In conjunction with Policy 91.004, the Authentication Credentials Complexity Standard establishes the standards for Ohio University credentials based on risk to the university.

These credentials will be maintained by the Information Security Identity and Access Management group, and reviewed on an annual basis by the University Data Stewards.

Risk Levels
These risk levels attempt to define, in broad categories, the levels of risk that different types of accounts present to the university. While the levels below have some examples of types of roles that would be included in the risk level, the role owners for the various roles at the university determine ultimately the Risk level that their role presents. An individual can always request that they be assigned a higher risk level than they would have by default. i.e., an individual may request to have risk level 4, and therefore multi-factor authentication, even if they are a student.

Risk Level 1
The lowest risk level to the University is for those individuals who only access their own information with their credentials, or only that information which is classified, by the University, or can reasonably be understood as “Low”, as defined by Ohio University Policy 93.001. Student and Guest accounts typically would fall into this category, barring access to additional resources.

Risk Level 2
The next lowest risk level to the University is for those individuals who have access to information which is classified, by the University, or can reasonably be understood as “Medium” or “High”, as defined by Ohio University Policy 93.001. Most university faculty and staff, as well as some students and guests, would fall into this category.

Risk Level 3
This risk level is identical to Risk level 2, but is available for those individuals that would prefer the corresponding Credential Level 3, identified below.

Risk Level 4
The highest risk level to the university is for those individuals who have privileged access to information that is classified by the University, or can reasonably be understood as “Medium” or “High”, as defined by Ohio University Policy 93.001. Some examples may include system administrators, network administrators,
database administrators, high-level functional users such as bursar, registrar, etc., and some application administrators.

**Standards for Credentials at Ohio University**

The credentials issued at Ohio University will conform to the following standards, based on Risk Level.

**Character Classes**
The four character classes referenced below are as follows:
1. Numbers
2. Upper Case Letters
3. Lower Case Letters
4. Special Characters (i.e. <:@#$%

**Dictionary Words**
Dictionary words are anything that exists in a list, or a dictionary in any language.

**Length**
This is the minimum number of characters for a password. The only maximum would be defined by any particular system in which the credential is used.

**Expiration**
Passwords must be changed within the timeframe defined under expiration

**Password Reuse**
Whether a previously used password can be used for the same account

**Credential Level 1**
Character Classes: 2+
Dictionary Words: No
Length: 8
Expiration: 5 years
Password Reuse: No

**Credential Level 2**
Character Classes: 3+
Dictionary Words: No
Length: 8
Expiration: 6 months
Password Reuse: No

**Credential Level 3**
Character Classes: 3+
Dictionary Words: No
Length: 10
Expiration: 1 year
Password Reuse: No

Credential Level 4
The Credential Level 4 standard is identical to Credential Level 3, with the addition of multifactor authentication (MFA). There are a variety of methods for achieving MFA, and as such, the Assistant CIO for Infrastructure Services and the University Information Security Officer must approve any particular method for MFA prior to its use.