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
## Revisions

<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.