Information Technology Department

Document Number: IT-SEC-0006.001
Document Name: Password Complexity Standard
Effective Date: 04/24/2018
Approval Date: 04/24/2018
Document Type: Standard
Page Count: 3
Document Status: Approved
Document Category: IT – Security
Document Owner: Lane Blanchard
Document Version: 1.0

1.0 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author(s)</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0</td>
<td>7/15/2013</td>
<td>UF IT Security</td>
<td>Initial UF Document that was adopted.</td>
</tr>
<tr>
<td>1.0</td>
<td>10/17/2018</td>
<td>Lane Blanchard</td>
<td>First full document drafted from adopted document; Modifications for internal needs and requirements</td>
</tr>
</tbody>
</table>

2.0 Approval

Name of Approver: Ian Tebbett
Title of Approver: Assoc. Dean, Entrepreneurial Programs and IT
Approval Date: 04/24/2018

3.0 Purpose

To define minimum password complexity requirements based upon assigned password policy levels.

4.0 Details

4.1 Password construction attributes (Table 1) for each password policy level are selected to achieve the specified minimum entropy.
4.2 Password composition rules require the inclusion of 3 of the 4 following character sets: lowercase letters, uppercase letters, numerals and special characters. Allowable special characters are ~ ! @ # $ % ^ & * ( ) _ + | - = \ { } ’ ” : ‘ < > ? , . / and the space character. Passwords may not include words of more than 4 characters, as tested against a dictionary of at least 50,000 words.

4.3 For all policy levels, the selection of a pass-phrase of at least 18 characters eliminates the password composition rules and dictionary check. Passphrases are subject to minimal tests to prevent use of common or trivial phrases.

4.4 Authentication token devices may be offered for use with policy levels P3-P5. When authentication token devices are used in conjunction with a password, the password is not required to comply with password construction attributes or composition rules.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
<th>P4</th>
<th>P5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Entropy Bits</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>31.5</td>
<td>31.5</td>
</tr>
<tr>
<td>Minimum Length of Password</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Maximum Age of Password (in days)</td>
<td>365</td>
<td>365</td>
<td>365</td>
<td>180</td>
<td>180</td>
</tr>
<tr>
<td>Password minimum age for reset (in days)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Password uniqueness / history (in days)</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>Failed attempts before lockout</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Lockout duration (minutes)</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
</tbody>
</table>

5.0 Scope

This policy applies to all passwords and other authentication methods used at the MTMCCC.

6.0 Related Policies

- IT-SEC-0006 Authentication Management Policy
- IT-SEC-0006.002 Authentication Management Standard

7.0 Definitions

No definitions needed for this standard.
8.0 Supporting Information

- NIST Publication 800-63 Electronic Authentication Guide