TABLE OF CONTENTS

1. STATEMENT OF POLICY .................................................................................................... 1
2. TO WHOM THIS POLICY APPLIES .................................................................................... 1
3. DEFINITIONS .......................................................................................................................... 2
4. POLICY .................................................................................................................................... 2
5. RESPONSIBLE ADMINISTRATOR ...................................................................................... 4
6. RELATED POLICIES .............................................................................................................. 4
7. HISTORY ................................................................................................................................ 4
8. SIGNATURE, TITLE, AND DATE OF APPROVAL ............................................................ 4

1. STATEMENT OF POLICY

This policy establishes standards regarding creation, protection, and security for passwords used on information systems maintained by Westminster College.

The purpose of this policy is to ensure the information systems maintained by the College are protected from unauthorized use.

2. TO WHOM THIS POLICY APPLIES

This policy applies to all users of information systems maintained by the College that require the use of a password or passcode; including students who are registered or enrolled for credit- or non-credit-bearing coursework (“students”); college employees, consisting of all faculty (full-time, part-time, adjunct faculty, and instructors) (collectively “faculty”) and staff (collectively “employees”); and contractors, vendors, visitors, guests, or other third parties (“third parties”).
3. DEFINITIONS

A. Contractors: Non-College employees who are working on behalf of the College on a temporary or on-going basis.

B. Employee: All faculty and staff who are employed by the College.

C. Faculty: Full-time, part-time, and adjunct faculty and instructors of the College.

D. Information Systems: Electronic systems that require the use of a password or passcode, are accessible on and/or off-campus, are used for official College business, and are maintained by the College.

E. Password and Passcode: A string of characters (letters, symbols, numbers) which may contain partial or whole words or sentences that are required to gain access to an information system.

F. Staff: Full-time and part-time staff.

G. Student: Students who are currently registered or enrolled for credit- or non-credit-bearing coursework.

H. Vendors: Non-college employees who are on campus for sales, consultation or product support.

4. POLICY

A. Creation of Passwords

1. The College requires the use of strong passwords to protect all user accounts. A strong password includes the following characteristics:
   a. Is greater than seven characters
   b. Contains no portion of your name or username
   c. Contains characters from three of the following categories:
      i. Uppercase letters of European languages (A through Z, with diacritic marks, Greek, and Cyrillic characters)
      ii. Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
      iii. Base 10 digits (0 through 9)
      iv. Non-alphanumeric characters (special characters) (e.g., , !, $, #, %)
v. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages

d. Is not a repeat use of an old password

e. Is not a dictionary word (e.g., “ALLIGATORS”)  
f. Is not a commonly used password (a list of commonly used passwords is available when you are changing your password)
g. Is not used on other systems on or off campus, e.g., a user’s Facebook account

2. Following are examples of strong passwords:
   a. “#brownsYUM” – Includes lowercase, uppercase, symbols, and is greater than seven characters
   b. “R00t4griffins” – Includes lowercase, uppercase, digits, and is greater than seven characters
   c. "CanRemb3r4ndTypeSentencesEasy!" – Includes uppercase, lowercase, digits, symbols, and is greater than seven characters

B. Protection of Passwords

1. The College uses “account lockout” to protect user accounts and prevent brute force attacks.

2. A user should not share a password with anyone:
   a. Do not share passwords verbally.
   b. Do not share passwords over email or other non-approved electronic means.
   c. Do not hint about your password to others.
   d. Do not share your password to colleagues, supervisors, or subordinates while on vacation.
   e. Do not share passwords in questionnaires or on security forms.

3. If someone asks for your password, refer them to Information Services security staff.

4. Do not write down your password or save it to a file on any electronic device without using encryption.

C. Security of Passwords

1. The College requires that passwords be changed frequently and are set to expire at regular intervals.

2. If a user suspects that an account is compromised, i.e., the password might be known to others, the user should report the incident to Information Services security staff and change the password immediately.
3. Anyone unable to abide by this policy should consult with the Director of Information Services and the Chief Information Officer to seek a policy exception. The Information Services security manager will keep a record of all approved exceptions and review them once a year.

5. RESPONSIBLE ADMINISTRATOR

Chief Information Officer is responsible for enforcing the Password Policy on behalf of the College.

6. RELATED POLICIES

None

7. HISTORY

<table>
<thead>
<tr>
<th>Date of Last Action</th>
<th>Action Taken</th>
<th>Authorizing Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 4, 2017</td>
<td>Interim Policy Adopted</td>
<td>Policy Governance Committee</td>
</tr>
<tr>
<td>May 5, 2017</td>
<td>Policy Adopted</td>
<td>Policy Governance Committee</td>
</tr>
</tbody>
</table>

8. SIGNATURE, TITLE, AND DATE OF APPROVAL

Approved: /s/_________________________________________

Stephen R. Morgan, President