1. PURPOSE

Westminster College maintains data essential and valuable to the performance of College business. These data resources are regulated by federal and state law as well as College policies that identify types of data and restrictions placed on data. This policy incorporates federal and state standards, regulations, and legislation, and establishes responsibilities for all forms of College data for confidentiality, integrity, regulatory compliance, and availability.

While data are critical to College operations and must be shared, data must also be used with care. The benefit of sharing data is greatly diminished through misuse, misinterpretation or unnecessary restrictions on access. Although some portion of the College data is public information, some data are restricted by federal or state legislation or by College policy. To comply with legislation and
protect the College community, the College has the right and obligation to protect, manage, secure, and control data under its purview.

2. TO WHOM THIS POLICY APPLIES

This policy applies to all faculty, adjunct faculty, staff, student employees, volunteers, contractor, affiliate, or duly authorized member of the community who can access College data.

3. DEFINITIONS

The following definitions apply to this policy. Terms not defined herein are defined in the Information Security Program Policy.

A. **Confidential Information**: Confidential Information includes, but is not limited to: any personally identifiable information, student and parent records, financial records (including social security and credit card numbers), and health records; contracts; research data; alumni and donor records; personnel records other than an individual's own personnel records; College financial data; computer passwords, College proprietary information/data; and any other information for which access, use, or disclosure is not authorized by: 1) federal, state, or local law; or 2) College policy or operations. Confidential Information includes either hardcopy or electronic information.

B. **Data Administrators**: College faculty and staff appointed by the Data Owner or ISO responsible for enabling user access and documenting users who have authorized access to a subset of data.

C. **Data Appeal Panel**: A panel comprised of the CIO, the cabinet member with oversight responsibility for the department or college with data under review, and a neutral party appointed jointly by the CIO and cabinet member. If any of these members has a conflict based on their participation in the underlying data decision, a cabinet member without a conflict shall serve on the panel for purposes of the appeal.

D. **Data Owner**: College faculty and staff with the responsibility to manage a subset of data (e.g., employee, student, financial, departmental, and research data, etc.) by establishing procedures and ensuring accuracy of all data within their area of responsibility.

E. **Data Processors**: Individuals that are authorized by data administrators to enter, modify or delete data.
F. **Data Users**: Any College employee, contractor, affiliate, or duly authorized member of the community who can access internal-use-only and/or confidential data but does not have access to modify or delete that data.

G. **Internal-Use-Only Data**: Data that requires protection against unauthorized disclosure, modification, destruction, and use, but the sensitivity of the information is less than that for Confidential Information. Examples of Internal-Use-Only data are internal memos, minutes, correspondence, and other documents whose distribution is limited as intended by the author.

H. **Legitimate Interest**: A need for access to internal-use-only or confidential data that arises within the scope of College employment and/or in the performance of authorized duties.

I. **Unrestricted Information**: Data that can be disclosed to any person inside or outside the College. Although security mechanisms are not needed to control disclosure and dissemination, they are still required to protect against unauthorized modification and destruction of information.

### 4. POLICY STATEMENT

A. General

Access to College data is provided to data users to conduct College business. Internal-use-only and confidential data, as defined by this policy, will be made available to data users who have legitimate interest. This may include data collected from students, faculty, adjunct faculty, staff, students, contractors, members of the community, or those who have no affiliation with the College. Data users accessing such data must observe the requirements for privacy and confidentiality, comply with the protection and control procedures, and accurately present the data used in any type of reporting. Data owners must establish internal controls to ensure that college policies are enforced. All data users are responsible for the security and privacy of the data they access as prescribed by this policy.

B. Compliance

1. The College forbids the disclosure of internal-use-only data or confidential data in any medium, including electronic information, hard copy information, and information shared verbally or visually (e.g. telephone or video), except as approved by the data administrator. The use of any internal-use-only or confidential College data for one’s own personal gain or profit, for the personal gain or profit of others or to satisfy personal curiosity is strictly prohibited.
2. Should a security breach occur or the misuse of College data be reported, the Incident Response Team will invoke an incident response process to investigate the facts related to the situation and determine the appropriate response. Disciplinary action will be taken in accordance with applicable regulations or College policy, up to and including termination or expulsion.

3. All individuals accessing College data are required to comply with applicable federal and state laws (e.g. FERPA, HIPAA) and College policies and procedures regarding security of confidential data and to exercise discretion with regard to such data. Any data user who engages in unauthorized use, disclosure, alteration, or destruction of such data in violation of this policy will be subject to appropriate disciplinary action, as described in section 7 below.

C. Responsibilities: Authorization for access to and the maintenance and protection of all College data, particularly confidential data, are delegated to specific individuals within their respective areas of responsibility. In some cases, one individual may serve in more than one role.

1. Data Owners
   a. Establish procedures and direction for the security and privacy of all College data and particularly confidential data within their respective areas of responsibilities.
   b. Ensure accuracy of all data within their area of responsibility.
   c. 

2. Data Administrators:
   a. Grant access to data for a legitimate interest as defined in this policy.
   b. Assign or configure access to College data as prescribed and approved by the data owner.
   c. Annually review access to all data and update access of users if necessary.
   d. Ensure that authorized data users understand their responsibilities with regard to their approved access.
   e. Maintain documentation of data users who have been authorized access to confidential data. Where an abuse of privileges is discovered, make access removal recommendations to the data owner.
   f. Work with the ISO to identify potential security gaps that may leave systems vulnerable to attacks or hacking and take remedial actions to make systems more secure.
   g. Report any possible breach in computer security or misuse of confidential or internal-use-only data to the Incident Response Team.
h. Ensure the usability, reliability, availability and integrity of information systems and the associated data.

3. Data Processor:
   a. Accurately input and present data. Data processors will be held responsible for their intentional misrepresentation of data.
   b. Maintain data integrity. Upon recognizing that any data elements are in error, the data processor will notify the appropriate data administrator.
   c. Report any possible breach in computer security or misuse of confidential or internal-use-only data to the Incident Response Team.

4. Data User:
   a. Use internal-use-only and confidential data only as required to perform the employee’s job responsibilities and as authorized.
   b. Respect and protect the confidentiality and privacy of individuals whose records to which they have access.
   c. Abide by federal and state laws and College policies and procedures with respect to access, use, and disclosure of confidential data.
   d. Report any possible breach in computer security or misuse of confidential or internal-use-only data to their supervisor, data owner, data administrator, or Incident Response Team.

5. TRAINING

All newly hired employees are required to complete training within 30 days of joining the Westminster community to understand their responsibilities under this policy. Thereafter, employees are required to participate in mandatory annual training and certification on the policy.

6. RESPONSIBLE ADMINISTRATORS

The ISO is responsible for oversight and administration of this policy. Among other responsibilities, the ISO shall classify data as confidential, internal-use-only, or public, and identify and appoint data owners. At least annually, the ISO will review the effectiveness of the policy and make any needed changes.

7. DISCIPLINARY SANCTIONS

Violations of this policy may result in sanctions and corrective actions up to and including termination and/or expulsion as set forth in the Staff Corrective Action Policy and Procedures, the Faculty Manual, and the Student Code of Conduct.
8. APPEAL PROCESS

A. Grounds

Within five school days of receiving notice of a decision denying access to data or notice regarding the classification of data which the individual disputes, the individual may submit an appeal in writing.

The grounds for appeal are the following:

- **Access to Data** – The individual has a legitimate interest for access to internal-use-only or confidential data based on the need to perform authorized duties within the scope of College employment.
- **Classification of Data** – The individual believes that the classification of data as confidential, internal-use-only, or public is inappropriate and should be changed.

Appeals of disciplinary sanctions must be made through the appropriate disciplinary process based on the status of the appealing party (faculty, staff, or student).

B. Appealing Party

To appeal a data decision, the appealing party must submit to the CIO a written statement citing the grounds for appeal and providing an explanation of their position. If the appealing party believes that the CIO has a conflict of interest to oversee the appeal, the party may submit the written statement to the general counsel who will appoint a neutral party to assume the duties of the CIO for purposes of the appeal.

C. CIO Duties Regarding Appeal

Upon receipt of a notice of appeal, the CIO will inform the ISO, data owner, and data administrator in writing of the appeal and assemble the Data Appeal Panel.

D. Data Appeal Panel

Within ten (10) school days of their being notified of the appeal, the Data Appeal Panel will meet at a mutually agreeable time to consider the information provided to them and to determine whether the data decision should be upheld. The appeal panel has the discretion to speak to the parties involved in reaching its conclusion but is not required to do so. The appeal panel will inform the ISO, data owner, and data administrator of the data decision in writing within five (5) school days of considering the matter.
E. No Further Appeal

The determination of the Data Appeal Panel will final and not subject to further review.

9. RELATED POLICIES AND PROCEDURES

- Confidentiality Policy
- Information Security Program Policy
- Data Governance and Access Policy Appendix A: Granting Access to College Data
- Data Governance and Access Policy Appendix B: Identification of Data Owners

10. HISTORY

<table>
<thead>
<tr>
<th>Date of Last Action</th>
<th>Action Taken</th>
<th>Authorizing Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 27, 2019</td>
<td>Data Governance and Access Policy Adopted</td>
<td>Policy Governance Committee</td>
</tr>
<tr>
<td>February 11, 2019</td>
<td>Interim Data Governance and Access Policy Approved</td>
<td>President’s Cabinet</td>
</tr>
</tbody>
</table>

11. SIGNATURE, TITLE, AND DATE OF APPROVAL

Approved: /s/ ________________________________
Bethami Dobkin, President