This Information Security Program serves as an umbrella program to provide a common organizational structure and approach to implementing and managing all policies that address information security at Westminster College.

2. PROGRAM ELEMENTS

A. The Information Security Officer (ISO) is appointed by the Chief Information Officer and serves as the chair of the Information Security Program Committee. The ISO is responsible for reviewing the Information Security Program periodically to ensure the program is staying abreast of changing technology and evolving risks, is maintaining compliance with Gramm-Leach-Bliley Act and the Federal Trade Commission Safeguards Rule, and is consistent with other existing and future laws and regulations. The ISO serves as the chair of the Incident Response Team. The ISO will also regularly review processes in other relevant offices of the College particularly as appropriate to any operational changes that may have a material impact on the program.
B. The **Information Security Program Committee (ISPC)** is charged with overseeing the security of the College’s non-public information (including information that is designated as confidential and/or sensitive either by applicable law or by the ISPC) through oversight and implementation of an overall Information Security Program that includes the policies listed in Section 3. Members of the ISPC are appointed by the ISO. ISPC members may include administrators from any College offices and departments as necessary to address issues before ISPC. The General Counsel and Chief Risk Officer work closely with the ISO and the ISPC and serve as resources on all elements of the Information Security Program.

C. The **Incident Response Team (IRT)** responds to technology security issues that arise. The response can vary, depending upon the seriousness of the event, the risk of further or additional damage, and the type of coordination and notification required. When computer security incidents occur, the IRT will handle all technology-based investigative and responsive actions in consultation with the General Counsel and Chief Risk Officer. The IRT’s responsibilities include:

1. establishing incident response plan and procedures;
2. testing the incident response plan annually;
3. holding incident response training session annually with team members;
4. providing annual review and familiarity with the business recovery and continuity plans;
5. maintaining an incident response emergency team contact list of those members that are available 24/7;
6. advising the ISPC on the nature of the breach/incident and possible courses of action;
7. maintaining data breach recordkeeping for breaches involving electronic data; and
8. performing preventive and predictive analysis to help mitigate against future threats.

D. The **Data Governance Committee (DGC)** is charged with the implementation and oversight of the Data Governance and Access Policy. The DGC creates data lifecycle, protection and retention plans, and coordinates the work of data owners. The DGC is chaired by the ISO and consists of the ISO and identified data owners.

### 3. POLICIES CONSTITUTING INFORMATION SECURITY PROGRAM

The following policies, which are administered as set forth in each specific policy, constitute the Information Security Program:
• California Consumer Privacy Act of 2018 (“CCPA”) (Policy No. 461) – Required by California law, imposes obligations on the College regarding how it controls or processes personal data about people who are located in California.

• Computing Resources, Network, and Email Use Policy (Policy No. 462) – This policy informs all users of the College’s computing and network resources of the authorized and proper uses of College-owned systems.

• Confidentiality Policy (Policy No. 463) – This policy informs all faculty, staff, student employees, and volunteers of their duty to protect and safeguard all confidential information acquired during the course of employment or service to the College.

• Data Governance and Access Policy (Policy No. 464) – This policy outlines the institutional governance for confidential information and builds an accountability framework for managing access and security for data.

• eCommerce Policy (Policy No. 465) – Consistent with the Payment Card Industry Data Security Standard (PCI DSS) requirements, this policy establishes requirements for accepting and transmitting credit and debit payment cards in the course of doing College business that will protect the cardholder’s credit data, uphold the College’s reputation, and minimize risk of financial costs resulting from a payment card data breach.

• Education Records Privacy Policy (Policy No. 466) - Required by the Family Education Rights and Privacy Act of 1974 (“FERPA”), this policy informs students and employees of the College of their respective rights and responsibilities including the circumstances under which the College may disclose student education records.

• Financial Information Security Policy (Policy No. 467) - Required by the Gramm-Leach-Bliley Act of 2003 ("GLBA"), this policy establishes certain practices related to safeguarding certain financial information to facilitate compliance with GLBA and the Federal Trade Commission Safeguards Rule.

• General Data Protection Regulation Policy (Policy No. 468) – Required by the European Union General Data Protection Regulation (“GDPR”), this policy imposes obligations on the College regarding how it controls or processes personal data about people who are located in the European Union.

• Identity Theft Policy (Policy No. 469) - Required by the Federal Trade Commission's Red Flag Rules under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), this policy codifies the College's procedures for identifying and responding to suspicious activity associated with accounts in which the College is acting as a creditor.
• **Password Policy (Policy No. 470)** – This policy establishes standards regarding creation, protection, and security for passwords used on information systems maintained by the College. The purpose of this policy is to ensure the security of the information systems by the College are protected from unauthorized use.

4. **HISTORY**

<table>
<thead>
<tr>
<th>Date of Last Action</th>
<th>Action Taken</th>
<th>Authorizing Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>August 27, 2019</td>
<td>Interim Information Security Program</td>
<td>President’s Cabinet</td>
</tr>
<tr>
<td></td>
<td>Policy Approved</td>
<td></td>
</tr>
</tbody>
</table>

5. **SIGNATURE, TITLE, AND DATE OF APPROVAL**

Approved: /s/________________________________________

Bethami Dobkin, President