1. STATEMENT OF POLICY

Westminster strives to empower end users to utilize technology to further the mission of the institution. We accomplish this through the acquisition and support of affordable and accessible technology that adheres to industry standards and best practices. Technology policies shall insure confidentiality, integrity, and availability of college resources. Systems and software will be implemented with consideration of business impact and resource constraints for all College divisions tasked with their implementation. This policy addresses account creation and user management to ensure the security and validity of Westminster College’s data and reporting through data visualization software known as Tableau.

2. TO WHOM THIS POLICY APPLIES

This policy applies to all faculty, staff, and students of the Westminster College community who have been approved to receive a Tableau account.
3. DEFINITIONS

A. Tableau Desktop: A data visualization software that makes databases and spreadsheets understandable to ordinary people.

B. Tableau Online: The ability to publish, share, and collaborate the designed visualizations in the cloud.

C. Site and Online Administrator: The person who is in charge of creating and maintaining the framework that enables Tableau Desktop users at Westminster College to publish, share, manage, and connect to data sources and workbooks. This person will centrally manage the data source permissions, credentials, access tokens, and refresh schedules for cloud-based data sources as well as the usage of published data sources and workbooks, and user activity. Site administrators have unrestricted access to the site’s content.

D. Tableau Desktop Account: These users will publish vetted data sources to the site that will be the shared data sources to which Tableau Online users can connect. Desktop accounts will also have an online account that uses the same login credentials. The College owns three desktop licenses and the Director of Institutional Research, Planning, and Effectiveness has assigned, and the President has approved, the individuals using the licenses.

E. Tableau Online Account: These users will connect to published, vetted data sources in the cloud. The College owns 13 desktop licenses and the Director of Institutional Research, Planning, and Effectiveness has assigned, and the President has approved, the individuals using the licenses.

F. TableauID: Based on the user’s email address, and provides unified, secure authentication to Tableau Online, the Tableau website, the Tableau Customer/Partner Portal, and the Tableau community forums.

G. Roles and Permissions: A role is a set of permissions that is applied to a project, workbook, view, or data source to manage user interaction. A wide range of specific permissions is available for each asset: view, create, edit, modify, delete, and more.

H. Content Permissions: A rule to specify who is allowed to work with which content resources on a particular site. Permissions are generally assigned to projects, workbooks, and data sources. Views in workbooks inherit permissions from the workbook, although you might have an edge case for which you want to set permissions for a single view.

I. Network Security: All communication between users and Tableau Online is encrypted using SSL for secure transmission of data. A variety of encryption techniques ensures security from browser to server tier to repository and back. In addition, Tableau has many built-in security mechanisms to help prevent spoofing, hijacking, and SQL injection attacks, and it actively tests and responds to new threats with monthly updates.

J. Application Security: The Tableau Online environment is hosted in a multi-tenant configuration providing separation of users, data, and metadata across customers.
K. Data Security: Tableau Online eliminates the need to implement VPNs or tunnels into your corporate environment. Many data sources can be captured as extracts and then refreshed on a regular basis. To use automatic refreshes, you need to embed credentials in the connection information for the data source.

L. You can define additional security in your workbooks and data sources by adding user and data source filters. Tableau also provides a User Filter capability that can enable row-level data security using the username, group, or full name of the current user. User filters allow you to set a filter on your data based on the identity of the person viewing the data.

4. APPLICABLE PROCEDURES UNDER THIS POLICY

A. Account Creation

There are two types of accounts created using Tableau:

1. Tableau Desktop Account (3): The default authentication type, TableauID, will be assigned to each user by the site administrator. Tableau credentials are made up of user name (email address) and password, which are stored in Tableau Online. Users enter their credentials directly on the Tableau Online sign-in page. Users must sign in explicitly each time they visit Tableau. The site administrator will create the TableauID, the user will receive an email invitation to the site, and the user will create a password. The accounts will be audited annually by the Director of Institutional Research, Planning, and Effectiveness, unless notified by Human Resources to terminate accounts to maintain appropriate access and for account deletion.

2. Tableau Online Account (13): The default authentication type, TableauID, will be assigned to each user by the site administrator. Tableau credentials are made up of user name (email address) and password, which are stored in Tableau Online. Users enter their credentials directly on the Tableau Online sign-in page. Users must sign in explicitly each time they visit Tableau. The site administrator will create the TableauID, the user will receive an email invitation to the site, and the user will create a password. The accounts will be audited annually by the Director of Institutional Research, Planning, and Effectiveness, unless notified by Human Resources to terminate accounts to maintain appropriate access and for account deletion.

B. User Security: The only people who have access to our site and content are the users who the site administrator has explicitly added to the site. If a user in no longer authorized in our system, the user’s account will be deleted by the site administrator.

1. User sign-in is secured by HTTPS
2. The password policy enforces strong passwords (PCI Compliant)
3. Accounts are locked for a period of time after repeated unsuccessful sign-in attempts
4. Accounts are validated by user email to prove identity
5. Passwords are stored using cryptographic protection, and no Tableau employee or contractor has access to plain-text passwords.

6. All local Tableau files and reports will be stored in a shared network file accessible by the desktop users only.

Tableau Online enforces a session timeout of two hours. After a short period of inactivity, users are signed out. Users will need to re-authenticate after not using Tableau Online for a period of 12 hours. These are Tableau Online system settings that cannot be modified.

C. User Permissions

The site administrator can set the following permissions:

1. Site roles: At the time a user is added to our site, a site role must be applied to them. This is the only setting applied to users (as opposed to content) to affect permissions. The site role determines whether the user can publish, interact with, or only view published content on that site. This will be assigned on an individual basis.
   
   a) Publisher: Publishers can sign in, browse the server, and interact with the published views. They also can connect to Tableau Online from Tableau Desktop to publish (upload) and download workbooks and data sources. Publishers cannot manage users.
   
   b) Interactor: Interactors can sign in, browse the server, and interact with the published views. They are not allowed to publish to the server.
   
   c) Viewer: Viewers can sign in and see published views on the server, but cannot use any interaction features like filtering and sorting. Users with site role can be allowed only to view and add and view comments.
   
   d) Unlicensed: Unlicensed users cannot sign in to the server. Users are assigned the Unlicensed role in the following circumstances:
      
      i. You import users from a CSV file
      ii. The number of available licenses is reached at the time you add or import users
      iii. You remove a user who owns content on the site. The user will still own the content but not be able to do anything with it.

2. Permission rules and templates: Content access is assigned through permission roles. These rules describe the capabilities you want a user or group to be able to perform on a set of content.

3. Content Ownership: By default, the person who publishes a data source or workbook to the server is the owner of that content. Ownership changes when another publisher updates the content on the server, or republishes it from Tableau Desktop. An administrator or project leader can change the ownership or set defaults for the project.
4. User permissions: The effective permissions that are the result of evaluating rules and settings, and which ultimately determine what a user can do with the content.

5. RESPONSIBLE ADMINISTRATOR

The Director of Institutional Research, Planning, and Effectiveness is responsible for enforcing the Tableau Account Policy and its related procedures on behalf of the College.

6. RELATED POLICIES AND PROCEDURES

A. SSAE 16 Report – Appendix A

7. HISTORY

<table>
<thead>
<tr>
<th>Date of Last Action</th>
<th>Action Taken</th>
<th>Authorizing Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 11, 2017</td>
<td>Interim Policy Adopted</td>
<td>Policy Governance Committee</td>
</tr>
<tr>
<td>February 13, 2017</td>
<td>Final Policy Adopted</td>
<td>Policy Governance Committee</td>
</tr>
</tbody>
</table>

8. SIGNATURE, TITLE, AND DATE OF APPROVAL

Approved: __________________________________________

Stephen R. Morgan, President