Work from Home Technology Policy
March 17, 2020

INTRODUCTION
A Virtual Private Network (VPN) is a secured private network that provides a secure encrypted connection or tunnel over the Internet between an individual computer/device and a private network such as the Belmont University Campus Network. Use of a VPN allows members of the Belmont community to securely access campus network resources from off campus as if they were on campus. For the purpose of this document, remote access is defined as any remote connection to a Belmont University network.

PURPOSE
The purpose of this policy is to state the requirements for remote access to computing resources and data hosted at the university using VPN technology.

SCOPE
This policy applies to all VPN users of computer and network resources owned or managed by Belmont University. Resources include all university owned, licensed, or managed hardware and licensed software. They also include the university network regardless of the ownership of the device connected to the network, the means of connecting, or the locale from which the connection is made.

POLICY
This policy provides the security requirements for all Belmont University employees who are manipulating and/or accessing university data classified by the Data Classification Policy as level 1 or 2 confidential information from remote locations using VPN technology.

This policy does not apply to authorized and authenticated access to email, MyBelmont, Blackboard, and/or any university publicly accessible websites.

REQUIREMENTS AND PRACTICES FOR ALL REMOTE USERS
Belmont employees and authorized third parties using the VPN must ensure that unauthorized users are not allowed access to internal university networks and associated information or data. All individuals and machines connecting remotely to university networks are subject to the university's Acceptable Use Policy.

All individuals connecting remotely shall only connect to or have access to machines and resources for which they have received permission and rights to use by the appropriate authorized university representative. All devices connecting remotely should be current on anti-virus software, operating system patches, and all application updates. Firewalls should be
enabled at all times.

**ADDITIONAL REQUIREMENTS FOR REMOTE WORK**

The machine/device must be trusted. This means that the machine/device must be built and maintained in a manner that creates confidence in the security of the machine. Home machines used for remote work should be used with caution when running applications prone to malware infections, such as peer-to-peer, gaming, and free (untrusted) software downloads.

Users are advised to avoid using their MyBelmont account and password or other university-related credentials on public or semi-public machines like Web kiosks.

The use of mobile devices to access email and other campus resources remotely should also be used with caution. Many of the same risks found with laptop and desktop computers apply to mobile devices. All mobile devices should employ a passcode at all times to protect access to the device.

All reasonable efforts must be made to protect university data keeping it in-house on secured servers and devices wherever possible. Users who connect remotely to university systems that contain confidential/restricted data are required by university policy to use the campus VPN to maintain security of university data.

Users needing remote access must use the VPN in conjunction with an approved remote access technology product. Users requiring VPN access must contact the Service Desk. The user’s remote access must be approved by the head of the unit/department approving them to work remotely.

**COMPLIANCE**

Violations of this policy will be handled according to normal disciplinary procedures. However, a user’s IT use privileges may be temporarily suspended by the Library and Information Technology Services (LITS) department prior to the initiation or completion of these procedures when there is a reasonable basis to believe that an individual is in violation of this policy.

Systems and accounts that are found to be in violation of this policy may be removed from the Belmont network, disabled, etc. as appropriate until the systems or accounts are in compliance with this policy.

**RELATED STANDARDS, POLICIES, AND PROCEDURES**

The Remote Access Policy is administered through a collection of Belmont standards. The Remote Access Policy and its standards are in effect at all times. LITS works in concert with the Dean of Students Office, Senior Leadership, and Human Resources to ensure fair and
appropriate investigation, consideration, and consequences where appropriate. Users are expected to familiarize themselves with Belmont standards and comply with them.

- Password Policy
- Acceptable User Policy
- Wireless Communication Policy
- Technology Purchasing Policy
- Data Classification Policy
- Belmont Bruin Guide
- 2020 Faculty Handbook
- 2020 Employee Handbook
- FERPA, HIPAA, GLBA Policies

**DEFINITION OF TERMS**

**USER:** Any person using any of the university’s computer or information resources including but not limited to:

- Students, Staff, Faculty, and Alumni
- Contractors and Consultants
- Visiting Staff
- Community Members and Guests
- Other users authorized by the university
- Third Parties (ex. Vendors, contractors, etc.)
- Anyone connecting non-Belmont equipment (e.g. laptop computers) to the university network

**LITS:** Library and Information Technology Services. Belmont division that supports library and technology services for the campus.

<table>
<thead>
<tr>
<th>Date of Change</th>
<th>Responsible</th>
<th>Summary of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 19, 2016</td>
<td>Randall Reynolds Director of Information Security</td>
<td>New Policy</td>
</tr>
<tr>
<td>Oct 20, 2016</td>
<td>Randall Reynolds Director of Information Security</td>
<td>Policy Update</td>
</tr>
<tr>
<td>May 12, 2017</td>
<td>Randall Reynolds Director of Information Security</td>
<td>Policy Update</td>
</tr>
<tr>
<td>March 17, 2020</td>
<td>William Ingram Chief Information Officer</td>
<td>Policy Update</td>
</tr>
</tbody>
</table>