MSU IT Data Center and Campus Network Remote Access Policy

This document will define the methods and requirements for access to the MSU IT Data Center Network or remote access to the campus network (“access”). The aim of these access classifications is to provide users with the same level of access to computing resources regardless of whether they are working on premise or remotely. Access requirements and methods will differ depending upon a user’s role and what their access requirements are.

Common data center and remote access methods include:
- Campus VPN (vpn-oncampus.montclair.edu / vpn-offcampus.montclair.edu)
- Bomgar Privileged Access Management (pam.montclair.edu)

All access will utilize encrypted protocols and may be monitored and audited. All access privileges must be granted via a request through the department of Information Security and Identity Management (ISIM). All activities in the MSU Data Center Network should follow the provisions set forth in the MSU IT Data Center Operating Guidelines.

When reading this document, it may be help to reference the MSU IT Access diagram.

This document will first summarize the different access scenarios, then define the user roles, access methods, and terms used in the access scenarios.

### Access Scenarios

<table>
<thead>
<tr>
<th>User Type (Linked to procedure)</th>
<th>Access Need</th>
<th>Requirements</th>
<th>Access Method</th>
<th>Request Process</th>
<th>Review &amp; Approvals</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MSU Authorized IT User</strong></td>
<td>Data Center Network</td>
<td>Client utilizing IT Managed/Secured image, MSU Privileged Account, 2FA</td>
<td>Campus VPN (AnyConnect)</td>
<td>MSU IT employee or manager submits request ticket</td>
<td>Dir. SIO ISIM Sec. Team</td>
</tr>
<tr>
<td><strong>MSU Authorized User</strong></td>
<td>Campus Network</td>
<td>NetID, 2FA</td>
<td>Campus VPN (AnyConnect, SSL VPN)</td>
<td>MSU employee submits request ticket</td>
<td>ISIM Sec. Team</td>
</tr>
<tr>
<td><strong>MSU Authorized Power User</strong></td>
<td>Data Center Network</td>
<td>MSU Privileged Account, 2FA*</td>
<td>Bomgar PAM</td>
<td>MSU employee submits request ticket</td>
<td>Dir. SIO ISIM Sec. Team</td>
</tr>
</tbody>
</table>

*2FA*: Two-Factor Authentication
A user’s privileges and methods of access will differ depending on their role in the organization, so it is important to have clearly defined user roles. Please refer to the [IT Privileged Account Policy](#) for specific information on the types of user accounts that will be assigned to the following roles.

**MSU Authorized IT User, Data Center Network**

MSU Authorized IT Users are IT personnel that require access to the Data Center Network. MSU Authorized IT Users must use their MSU Privileged Account with two-factor authentication and the Cisco AnyConnect client running on an MSU managed workstation. These connections will be terminated in a Privileged Network that provides direct access to the Data Center Network.

**MSU Authorized User, Campus Network**

MSU Authorized Users are essentially non-IT personnel that require access to the Campus Network. Authorized Users must use their MSU NetID with two-factor authentication, and should be allowed to use the AnyConnect client or an SSL VPN connection from any machine. These connections will be terminated in an Unprivileged Network that does not have direct data center access, and may have certain access restrictions.

**MSU Authorized Power User, Data Center Network**

MSU Authorized Power Users are essentially non-IT personnel that require access to hosts on the Data Center Network. Authorized Power Users must use a MSU Privileged Account with Bomgar PAM in combination with a two-factor authentication. Bomgar PAM can provide direct access to the specific machines these users need access to.

**MSU Authorized Vendor or External (non-NetID) Users, Any Network**

MSU Authorized Vendor or External Users without NetIDs that require access to hosts on the Data Center Network or Campus Network must use a MSU Privileged Account with Bomgar
PAM in combination with two-factor authentication. Bomgar PAM can provide direct access to the specific machines these users need access to. (Users will be provisioned a non-NetID account (not an affiliate NetID), to facilitate authentication.)

Two-Factor Authentication (2FA)
A second factor of authentication is required in all access scenarios. 2FA protects user credentials by requiring a second factor, typically an app on a mobile phone or an SMS message. The 2FA solution used for various services is approved by the Director of ISIM.

Managed Workstation
An MSU managed workstation that is running the most recent version of the Windows or Mac IT Secured/Managed Image is required when an MSU Authorized User is connecting to the Campus VPN in order to connect to data center resources.

Access Methods

Campus VPN
The Campus VPN provides access to certain users and places them in specific networks based on their role. Access to data center hosts is then to be defined by the access privileges of these networks. All access to the Campus VPN requires enrollment in a two-factor authentication solution. Requests for access to the Campus VPN should be submitted to the ISIM group via an Incident in ServiceNow using the Data Center and Campus Network Access Request template.

Bomgar Privileged Access Manager (PAM)
Bomgar PAM provides monitored privileged access to MSU Authorized Power Users and MSU Authorized Vendors or External (non-NetID) Users. Bomgar PAM can be accessed from both off campus and on campus. Requests for access to Bomgar PAM should be submitted to the ISIM group via an Incident in ServiceNow using the Data Center and Campus Network Access Request template.

Network Definitions

Data Center Network
The Data Center Network is a group of Virtual LANS (VLANs) used by data center hosts. This network is separated from the Campus Network via the Data Center Firewall. The network includes separate VLANs for MSU Servers, Finance Servers, Student Information Systems Servers, and Infrastructure Servers.

Privileged Network
The Privileged Network is a group of VLANs where privileged connections from the Campus VPN are terminated. Machines contained here are allowed access to data center hosts.
Campus Network
The Campus Network is a group of VLANs for general campus use, and includes any publicly available hosts. Users on the Campus Network are not allowed to access the data center but can be allowed access by request to data center resources via the Bomgar Privileged Access Management (PAM) appliance.