What Device Can I Use for UMBC Work as a Staff or Faculty Member?

As a UMBC staff or faculty member, it is essential that you take appropriate steps to protect university information.

**If you have any questions about devices you want to use or how to classify information, please contact the DoIT Security Department at security@umbc.edu.**

**It is better to ask before possibly causing an information breach.**

Information Classification

University information is broadly categorized into one of four levels.

- **Level 0 - Public Information**
  - Level 0 information is information that is public to the world and not subject to any laws or restrictions on who can access it. This information could be posted on a billboard anywhere in the world, and it would be no problem.

- **Level 1 - UMBC Proprietary Information & FERPA**
  - Most of the information used as a part of the academic and business processes of UMBC is Level 1 data. This includes any information that is covered under FERPA and any information that is related to UMBC business or academic programs, that isn’t covered by another law or contractual restriction.

- **Level 2 - Confidential Information**
  - Level 2 information is any information that could be implicated in a data breach under identity theft laws. This includes information such as:
    - Social Security Numbers
    - Drivers License Numbers
    - Passport and VISA Numbers
    - Credit Card Numbers (for non-UMBC credit cards)
    - Financial Account Numbers (for Financial Accounts Outside of UMBC)

- **Level 3 - High Security Information / Legal Protections Required**
  - Level 3 data is our highest classification of general information at UMBC. This level includes information that must be protected specifically under state, federal, or international law. The main law that falls under this category is health information that is covered by HIPAA.

Permitted Devices by Information Classification

The way that we need to secure the information depends on the level of the information. The higher the level, the more security we need to apply to the information. When trying to determine which types of device can be used with which types of information, please consult the following matrix.

The device must match the highest level of information on the device. For example, if a computer is regularly used with Level 1 information and has only a few Social Security numbers on it for a one-time task, the whole device must match the higher Level 2 requirements (due to the SSNs), or the SSNs must be removed from the computer.

**It is always better to use a UMBC Owned Device or the UMBC Virtual Desktop Environment whenever possible, even with Level 0 and Level 1 Information.**

<table>
<thead>
<tr>
<th></th>
<th>Level 0</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>UMBC Owned Device</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes**</td>
<td>Yes**</td>
</tr>
<tr>
<td>UMBC Virtual Desktop Environment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Employee Owned Device</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Public Device</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

** The UMBC Owned Devices need to have particular security configurations and tools installed to be able to work with Level 2 and Level 3 information.

For information on using the UMBC Virtual Desktop Environment, please review the following FAQ: UMBC VDE