OM 9.1.4 - Device Security

[ Scope ] [ Reason for Policy ] [ Policy Statement ] [ History ]

About This Policy

<table>
<thead>
<tr>
<th>Effective Date: April 1, 2017</th>
<th>Policy Contact:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Updated: March 6, 2018</td>
<td>Office of Information Technology</td>
</tr>
<tr>
<td>Responsible University Office: Office of Information Technology</td>
<td><a href="mailto:helpdesk@clarkson.edu">helpdesk@clarkson.edu</a></td>
</tr>
<tr>
<td>Responsible University Administrator: Chief Information Officer</td>
<td></td>
</tr>
</tbody>
</table>

Scope

All Clarkson University units and employees.

Reason for Policy

As technology advances, data can be received, transmitted, processed and stored on an ever-increasing array of devices. The Device Security Policies outline specific requirements for broad classes of devices.

Policy Statement

Regardless of the device type, reasonable steps must be followed to protect the confidentiality, integrity and availability of the data residing on and transmitted through electronic devices. Generally speaking, all devices must:

- Be protected by an access-authorization mechanism such as PIN or username/password combination
- Have encrypted storage devices where applicable
- Must not be left in a location that permits casual, unapproved physical access to the device
- Must not be configured to permit casual, unapproved network access to the device

Specific practices and requirements of broad categories of devices are included as sub-policies within the Device Security policy.

History

March, 2018