Administrative Laptop Policy

This policy covers all laptops that are provided access to College administrative systems (i.e. MSOL, Banner, IFMS, etc.) through a College administrative connection. This policy does not include college laptops that only have access the Public wireless network. Administrative laptops will have access similar to college desktops on the administrative network. As such, at minimum, they require the same security systems in place.

- Administrative laptops must be members of the College Administrative domain.

- Administrative laptops will be set up with the standard College administrative [1]image by Desktop Support and will include the following:

    - The standard anti-virus software;
    - The standard agent to manage the anti-virus software;
    - The standard management agent used by the College to keep systems up to date; and.
    - Standard scripts necessary to allow the College's IT services to ensure security, which shall be automatically set to run at startup, shutdown or when any other programs installed.

- Administrative laptops will utilize full disk encryption in accordance with the College's Encryption and Key Management Standard.

- As with College administrative desktops, individuals are <u>not</u> provided administrative rights on these units.

- Administrative laptops are provided to individuals for a variety of reasons. Those provided for desktop replacement are expected to be available at work whenever the individual is on campus. At the minimum, each laptop must be turned on and connected to the College wireless network at least once each week to receive software and patch updates. Instructions accompanying updates must be followed. These may include multiple reboots to apply downloaded patches.

- Periodically these laptops will need to be updated by Desktop Services. Individuals provided administrative laptops on loan must return the laptop to Desktop Services when requested for changes and updates.

- Each laptop user must execute their first time login at the College, authenticating through the College Administrative domain. Subsequent logins can be executed off the network/site.

[1] The College does not have administrative images for all laptops. As a result, the laptop models that can be set up for administrative purposes are limited. In particular, access for older models may not be possible.

- As with all College systems, logins are not to be shared with others and laptops are not to be used by unauthorized individuals.

- For on campus access to College administrative systems, these laptops will be set up and registered to connect via the College's wireless administrative network using the [2]standard methodology implemented by Networking and Telecommunications.

    - In the standard setup, administrative laptops will not be registered for access to the SCCC-Public wireless network. Specific needs for this connection will be evaluated by Networking and Telecommunications or Desktop Services.

- All access to College data and systems in all locations will be handled through the College's VPN client connection. This provides an encrypted, managed connection from the laptop through whatever route is used to reach the College's administrative network. Examples of College data and systems include IFMS, INB Banner, College files on administrative servers and My Documents.

- Individuals will use Outlook's Web Client to access College email. The Outlook desktop client will not be configured.

- Laptops are more susceptible to loss and theft. Accordingly, individuals must observe higher security precautions when downloading and using critical or private College data on these devices and must make every effort to ensure the continued confidentiality of that data.

    - Do not use the laptop in a manner that allows unauthorized individuals to view private College data.
    - Do not leave the laptop unattended when in use and secure the laptop when it is not in use.
    - If the laptop is misplaced or stolen, immediately notify Desktop Services.

- Individuals should avoid keeping copies of files on the laptop. Once the laptop is connected to the College via VPN client, files should be moved from the laptop to the network-based My Documents folder.

- As with all administrative systems, installation of additional software must be requested through Desktop Services. Software will be reviewed for conflicts with College applications and must be cleared prior to installation. Proof of license is required.

---

[2] At the current time the connection will be available through a wireless network adapter with DHCP enabled. In some cases, hard coded IP addresses may be deemed necessary by the Office of Computer and Information Systems.