

Administrative Policies

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.

lMops

- 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 the²standard 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