900.11 Cellular Phones & Mobile Device Management

900.11.a Cellular Phone

Cellular phones and other wireless communications devices, such as those allowing access to the University's online resources and internet, are provided to improve employee productivity and customer service, and to enhance business efficiencies. Cellular phones are not provided for primarily personal benefit. Before receiving a University-subsidized device or service plan, it must be established that the employee has a business need for the device, and an appropriate service plan must be approved by the employee's department head or administrative supervisor. University issued mobile devices are susceptible to use for personal purposes and a reasonable amount of personal use may be permitted.

Employees assigned a cellular phone are expected to have it on or near their person during working hours, to keep it turned on, and to respond to all calls made to them. Conversations should be kept to a minimum. Use of personal cell phones during business hours should be kept to a minimum. As with telephone usage, the image and disruption to work must be taken into consideration.

All university employees and associates who are authorized by their department heads to obtain a mobile communications device and related services that will be paid for with University funds, and to those who elect instead to receive a monthly allowance to cover the business use of their own, personal mobile devices and accounts are expected to abide by the Mobile Communications policy. The policy in its entirety may be located on the Office of Policy and Compliance website in the Colorado State University Policy Library.

900.11.b

Mobile Device Management

It is the department's responsibility to protect University assets. To do this the department is using mobile device management software in order to support and maintain laptops, tablets, cell phones and any other mobile devices. This software allows the department to remotely install and update applications on devices (as well as manage the licenses for these apps), unlock devices when the passcode is forgotten, find lost or stolen devices, and when a device is lost or stolen and cannot be retrieved, the device can be remotely erased.

Such software will only be installed on department owned devices. It will not be installed on any device that is personally owned even if it is used for University business.

Once installed, it is the employee's responsibility to leave the application installed and not remove or change the application. Removal or changing the application will be reported to the supervisor for appropriate action and the device will be returned to compliance.