Draft Rutgers Connect MDM Standard
OIT
Revised 8/28/2016

Mobile Device Management, MDM, is a service that is part of Rutgers Connect (Office 365) and is used to assist in managing mobile devices. This proposed standard applies to managed Rutgers owned and personally owned mobile devices that connect to Rutgers Connect (Office 365). The purpose of this standard is to safeguard Rutgers data on mobile devices, particularly if mobile devices are lost or stolen. There are two distinct standards:

1. Basic MDM Standard – this is to be applied to all Rutgers owned and personal devices that are used by faculty, staff, guests and students who do not handle HIPAA or other restricted data. This enforces the following rules for a mobile device connecting to Rutgers Connect:
   a. Device must have a password. This can be a simple 4 digit numeric pin and/or thumbprint or other secure login technologies.
   b. Device must allow for a remote wipe.

2. MDM Standard for People Handling Restricted/HIPAA data – this is to be applied to all Rutgers owned and personal devices that are used by faculty, staff, guests and students that handle HIPAA or other restricted data. This enforces the following rules for a mobile device connecting to Rutgers Connect:
   a. Device must have a high level password made up of alphanumeric characters, one special character and a minimum of 6 characters in length.
   b. Device must be encrypted.
   c. Device must allow for a remote wipe.
   d. If mobile devices are lost or stolen, the device will be wiped at request of the owner of the device.
   e. 10 or more consecutive login failures by the user of the device will cause the device to be wiped (erase all data on the device).

Use of Personal Devices (BYOD): If a user declines to allow Rutgers MDM on their personal mobile device, there are several restrictions that still need to be followed if planning to access Rutgers data. The personal mobile device should be configured to not allow the storing of data locally, that is residing in Office 365 or any other restricted data on their mobile device. Further the user is still responsible for securing the mobile devices as per the applicable guidelines, including setting a pin on their devices to prevent unauthorized access as per the set of minimum security standards outlined here: https://rusecure.rutgers.edu/content/minimum-security-standards-data-protection. Users may still access Rutgers Connect using a web browser on their mobile device and connecting via OWA (web interface). Accessing Rutgers Connect with OWA allows access to basic email and calendaring, while minimizing the caching of data locally on their mobile device.

All personal devices used for University business must adhere to the security and management requirements of this standard and the Acceptable Use Policy (AUP). See: http://policies.rutgers.edu/sites/policies/files/00005571.PDF. One should not attempt to circumvent security procedures of these policies and standards.