How do I protect University information that might be accessible on my personally-owned Mobile Communication Device (MCD) if it is lost or stolen?

Tell Me
Supplemental to University Policy 602.10, Mobile Communication Device Allowances and MCD Procedures.

1. If your mobile device has been set up to synchronize with the University’s server to receive mail and is lost or stolen, you can issue a remote device wipe command to protect your data.
2. This command erases all data on the mobile device including all synchronized information and personal settings, returning the device to the original factory settings.

Info
Visit the ITS Guideline for Mobile Devices for more information on protecting university information resources from unauthorized access or disclosure when using mobile devices.

Related articles
- Can our Department create policies to ensure that FLSA (Fair Labors Standard Act) subject employees who receive a Mobile Communication Device (MCD) allowance do not use their devices outside of normal, established working hours?
- Are there specific security policies I need to comply with if I receive a Mobile Communication Device (MCD) allowance for my personal MCD?
- Is an employee on leave eligible to receive an MCD allowance?
- How do I terminate an MCD allowance?
- What supporting documentation should I submit with my MCD Allowance Request eForm?