Procedures and Implementation Information for Bring Your Own Device (BYOD) and Mobile Devices

1. The use of mobile computing/storage devices to access CI is a privilege that may be revoked at any time, and not a right;

2. CI will be accessed through networks using procedures established by IT. This may include the use of secured network connections, the use of College-approved Virtual Private Network (VPN) services using username/ password credentials, and/or other relevant methods as provided by IT;

3. For personally-owned devices, users will obtain and install the latest security and operating system updates from the device vendor as well as any software required to access the network;

4. All applicable security options available on the device will be utilized to the greatest practical extent, such as, but not limited to: passwords, firewalls, encryption and anti-virus software. At a minimum, mobile computing/storage devices that access the College's CI must be password protected;

5. IT may restrict the access of a mobile computing/storage device if the device presents a suspect or demonstrable threat to the integrity of CI or other computing resources;

6. Avoid storing CI whenever possible on personal mobile computing/storage devices, and delete CI when no longer needed on such devices;

7. The transfer of CI to mobile devices that do not comply with this policy is prohibited;

8. Any device containing CI may be subject to seizure under applicable laws or in response to a court order, such as a subpoena;

9. When a possible security breach is investigated as required under the law, personal mobile computing/storage devices may need to be provided to law enforcement or IT for evaluation;

10. In the event that a device is lost or stolen which is suspected to contain CI, the College reserves the right to remotely disable and erase (wipe) all data on the device;

11. The College will not make exceptions or supply additional provisions to support personally-owned devices that are unable to connect to the network;

12. Users hold the College harmless for damage to personally owned-devices and related software resulting from use of the College network, and from the loss of any personal data contained on the device;

13. Upon termination, resignation, or retirement from employment, users shall remove from personal mobile computing/storage devices all CI obtained from the College that contains the below data elements, and inform their supervisor that the information has been removed:
    (1) social security number;
    (2) driver's license number or non-driver identification card number;
    (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
14. In the case of a failed personally-owned mobile computing/storage device on which was stored CI obtained from the College that contains:
    (1) social security number;
    (2) driver's license number or non-driver identification card number;
    (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

    Users shall inform their supervisor that the device has failed and that the information is no longer accessible. It is recommended that the supervisor contact IT to review the device and assist in determining proper disposal.