DUQUESNE UNIVERSITY
Computing and Technology Services

| Mobile Device Service Requirements | Effective Date: 7/1/2018<br>Responsible Officer: Charles Bartel, Vice President for Information Technology and Chief Information Officer |
|---|---|

## 1. Purpose:

This Service Requirement defines the appropriate use of mobile devices as a means of accessing Restricted or Internal University Data. This service requirement's purpose is to provide the ways in which the University permits the use of mobile devices to access University data.

These service requirements apply to any mobile device that accesses Duquesne University Data. It also applies to any campus affiliates including faculty, staff, students, retirees, or guests accessing University Data.

University Data that is considered Restricted or Internal is defined in the CTS Data Governance Service Requirements detailed at http://duq.edu/about/campus/computing-and-technology/policies/service-requirements/cts-data-governance-.

## 2. Service Requirements:

These Mobile Device Service Requirements specify the fundamental details for the appropriate use of mobile devices at Duquesne University.

a. University Owned Mobile Devices:

Certain University employees are required to use mobile devices for Duquesne University business functions. University supervisors must identify those employees that require a mobile device as part of their job responsibilities. Computing and Technology Services (CTS) is responsible for the procurement and institutional management all University owned mobile devices. CTS will work directly with IT support staff, departments and individuals on the purchase of a mobile device and any subscription to data/voice plans. Departments are responsible for providing the appropriate funding for the purchase of the devices and subscriptions to voice/data plans.

All University-owned mobile devices are required to be managed by Computing and Technology Services (CTS), which requires the installation of managed service software. This software allows the University to maintain proper security controls, software updates, approved applications, and configurations of mobile devices owned by the University.

Employees are allowed incidental personal use of University-owned mobile devices as long as no applicable fees, state or federal laws and/or university policies are being violated by such use. University-owned mobile devices including the data stored on a device, and the data/voice plans and records are sole property of the University. When an employee leaves

the University, all University-owned mobile devices must be returned to the University.

b. Personally Owned Mobile Devices:

The University recognizes that in today's world of mobile devices, many individuals leverage the use of their personal mobile devices to connect to University information technology resources. Computing and Technology Services (CTS) permits the use of personal devices to access certain resources on campus, but may require security controls be configured on personal devices based on the sensitivity of that data that individuals are accessing. All use of personally owned devices to access University Data must comply with state and federal laws, as well as with Duquesne University's own policies and service requirements governing the appropriate use of technology.

c. All Mobile Devices accessing University Internal or Restricted Data:

If a campus affiliate, either for work-related or academic requirements or through their own personal choice, elects to access University Data via a mobile device, they must accept the security policies defined by the University. These security policies will be required to be added to the mobile device upon connecting to University Data.

The mobile security requirements to access University Data are:

- Require at least a 5 digit pin/passcode to unlock the device;
- Access to remotely wipe the Duquesne University data in the event the device is lost or stolen;
- Potentially limit the amount of email that can be stored on the device based on manufacturer/software availability.

Data Loss Prevention (DLP) continues to be a concern at Duquesne and other institutions across the world try to gain control over the proliferation of sensitive data and how to put policy and controls around it. Data breaches continue to affect institutions, resulting in tarnished reputations and costly identity protection services. It is important that members of our community be aware of the restricted data including personally identifiable information (PII) that might be stored on devices, and remove any traces of PII immediately.

Report a Lost or Stolen Mobile Device Processes:

- If a University-owned or personal mobile device containing University Data classified as Restricted or Internal is lost or stolen, please contact the CTS Help Desk at 412-396-4357 to report the device is missing. CTS may then issue a remote wipe command to erase the University data from the mobile device.

d. Other Best Practices for mobile device management:

While not requirements, these best practices for mobile device management will help provide our campus affiliates guidance on how to protect and secure mobile devices.

- Use anti-malware application.
- Leverage encryption if possible.
- Verify encryption mechanisms and ensure that data is being transmitted securely.
- Disable options and applications that you don't use.
- Regularly back up your data.
- Dispose of your device safely by removing all sensitive data.

- Avoid jailbreaking.
- Verify applications before downloading.

### 3. Enforcement:

The unauthorized or improper use of Duquesne University's technology environment, including the failure to comply with these service requirements, constitutes a violation which may result in the loss of access, University disciplinary actions and/or legal prosecution under federal, state and local laws, where applicable. Users are expected to adhere to T.A.P. 26 - Computing and Ethics Guidelines which can be found at http://www.duq.edu/taps.

The University reserves the right to amend these service requirements at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with other published policies and with applicable federal, state, and local laws.

| Revision Date | Reason for Change | Author |
|---|---|---|
| 7/1/2018 | Initial Draft | Tom Dugas, Chief Information Security Officer |
| | | |