University of Portland

Mobile Device Policy

1. **PURPOSE:** The purpose of this policy is to define standards for secure mobile device use including the use of University owned mobile devices while off campus and connecting personal or University owned mobile devices to the University of Portland's network or applications. These standards are designed to minimize the potential exposure to the university from damages which may result from unauthorized use of university resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical university systems, etc.

2. **SCOPE:** This policy applies to all University of Portland employees, contractors, vendors and agents with a university owned or personally owned computer or device used to connect to the university of Portland network and applications. This policy applies to remote connections to the university network and external internet connections used to do work on behalf of the university, including reading or sending email and utilizing university supplied cloud applications.

3. **POLICY:**

   a. **Employee Access:** It is the responsibility of University of Portland employees, contractors, vendors and agents with remote access privileges to the university network to ensure that their remote access connection is given the same considerations as the user's on-site connection to the University of Portland.

   b. **Non-employee Access:** Access to the internet for recreational use by immediate household members through the University of Portland's network on personal computers is permitted for employees that reside on campus. The employee is responsible to ensure the family member does not violate university of Portland policies, does not perform illegal activities, and does not use access for outside business interests. Use of University supplied devices is strongly discouraged for household use by family members. The university employee bears responsibility for the consequences should access be misused.

   c. **Physical Device Security:** Mobile devices should never be left unattended and unsecured. If a device is left unattended, it must be out of sight in a locked space (e.g., desk drawer, file cabinet drawer, locked office space, hotel safe, etc). If a device cannot be locked inside a secure location, it must be physically secured to an immovable object with a security cable or kept on your person. Technical Support staff can assist with procuring locking cables and other security devices. **NEVER LEAVE UNIVERSITY ISSUED DEVICES UNATTENDED IN A VEHICLE OR HOTEL ROOM (other than in locked safe)**.

   d. **Local Data Security:** Mobile devices should not store any university information of a Level 1 or Level 2 classification as defined by the *Data Risk Classification Guidelines*. Devices that use desktop-class operating systems (Windows, Mac OSX, etc.) must be secured with your University login credentials. Under no circumstances shall a logon password requirement be removed or bypassed. For devices with a mobile operating system (Apple iOS, Android, etc.) a passcode or PIN code must be enabled to access the device.

   e. **Network Connectivity:** The university will implement and maintain wireless access controls to protect system resources from unauthorized access. Wireless resources will be managed, maintained and

controlled by the universities Information Services group using end-to-end encryption establishing a virtual private network between the wireless workstation and other devices on the network. Access to wireless resources, outside UPGuest, will be restricted to encrypted sessions and UP issues accounts.

f. **Lost, Damaged or Stolen Devices:** Any devices or accessories that are lost or stolen will be replaced per the *Theft or Loss Policy*.

g. **Disposal of Equipment.** University of Portland equipment must be returned to Information Services for proper disposal. Devices will be securely scrubbed per the Information Security Policy.

h. **Specialized Access:** Organizations or individuals who wish to implement non-standard Remote Access solutions to the University of Portland's production network must obtain prior approval from the Chief Information Officer (CIO).

4. **GUIDANCE:**

a. **Connecting devices to the UP network**: Mobile devices must be protected with a password or PIN. Devices must have up to date antivirus/malware and firewall protection enabled. Location services must be enabled for university owned devices at all times.

b. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

c. At no time should any University of Portland employee provide their login or email password to anyone, not even family members.

d. University of Portland employees and contractors with remote access privileges must ensure that their university owned or personal computer or workstation, which is remotely connected to University of Portland's network, is not connected to any open wireless networks, with the exception of personal networks that are under the complete control of the user.

e. University of Portland employees and contractors with remote access privileges to the university's network must not use non-university email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct University of Portland business, thereby ensuring that official business is never confused with personal business.

f. All devices or applications that are connected to University of Portland resources must conform to the policy.

5. **EXCEPTIONS:** In the unlikely event that a system cannot conform to this policy, the appropriate director will inform the Vice President for University Operations and detail the specific actions being taken and/or resources needed to comply with the intent of this policy.

6. **SANCTIONS:** Accounts and network access may be administratively suspended by the University with or without notice when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy. Any violation of this policy by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of student status. Faculty and staff violations will be addressed by their

respective disciplinary policies and procedures. All known and/or suspected violations will be reported to the Vice President for University Operations. Users of University of Portland computing facilities are subject not only to University Policies, but also to applicable local, state and federal laws.