Personally Owned Computing Device Standards - University of Massachusetts President's Office

I. Purpose:

The purpose of these standards is to define the appropriate use and procedures for using Personally Owned Computing Devices (POCD's) on the UMASS President's Office (PO) network.

II. President's Office POCD Network Usage Standard:

President's Office Employees & Consultants/Vendors with UMASSP system credentials while on President's Office premises:

- Non-UMASS provided laptops are not permitted on secure PO networks (networks requiring user authentication).
- POCD's such as tablets, IPADS, Cell Phones are permitted on the PO provided wireless networks.
- PO employees may use Non-UMASS provided phones on the PO wireless network to access Exchange (e.g. UMASSP Email), providing the phone is protected with a PIN/Password.
- Any exceptions to this standard must be applied for via an email request to: helpdesk@umassp.edu. POCD's requiring exceptions will need to verify security equivalence to devices provided by the President's Office. This includes up to date anti-virus and malware software has been properly installed and the use of the device being consistent with all President's Office provided devices and policies.

Non-President's Office Employees while on President's Office premises:

- Members of the Eduroam access service may utilize the provided Eduroam wireless network, all other users will use the Guest wireless network.

All President's Office Network Users:

- At no time does the University accept liability for the maintenance, backup, security, or loss of personal data on a personal device.
- The University shall **NOT** be liable for the loss, theft, or damage of POCD's.
- POCD's are part of a rapidly changing technology and UMASS reserves the right to modify this standard. UMASS IT may elect to implement additional requirements or processes to safeguard the University's Computing Resources. The most current version of this standard will be posted on the https://www.umassp.edu/central-admin-guidelines website.

User Responsibilities:

- UMASS Personally identifiable information (PII) data shall not be stored on any personally owned computing devices.
- Notify the UMASS President's Office HelpDesk (helpdesk@umassp.edu) of any theft or loss of a POCD containing data or software application licenses belonging to the President's Office.
- PO employees may use Non-UMASS provided phones on the PO wireless network to access Exchange (e.g. UMASSP Email) providing the phone is protected with a PIN/Password.
- At no time should a POCD be used to conduct any point of sale transactions on behalf of the University. For assistance with taking debit & credit card payments on a University owned device, please refer to Treasurer's Fiscal Procedure No. 08-01, and the Administrative Standards for the Treasurer's Fiscal Procedure No. 08-01, Merchant Debit and Credit Card Receipts documents.
- When downloading applications, verify that the application is from credible sources to reduce the risk of introducing malware.
- Keep your personal device current with patches and updates to avoid any security vulnerabilities.
- Ensure your personal device has anti-virus protection.
- Never retain UMASS sensitive or confidential data e.g. PII, FERPA, HIPPA, PCI/DSS, etc.
- Apply auto screen lock settings to any personal device.

Security:

The President's Office IT organization reserves the right to monitor and perform security scans on any personally-owned device that accesses President's Office networks. IT may, without notification, prevent or ban POCD from the President's Office network which disrupt any University Computing Resources or are used in a manner which violates any University policies.

III. Enforcement:

Failure to comply with the President's Office POCD standard may, at the full discretion of UMASSPO, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and/or possible termination of employment.