Homewood Student Affairs

Computer Hardware Procurement Policy

The intent of the HSA Computer Hardware Procurement Policy is to provide staff with reliable, technically capable and secure computing access.

1) General guidelines
   a) Procurement of new desktop or laptop hardware is normally funded centrally from the HSA Finance Operations office
      i) Staff member will receive either a desktop or laptop with docking station based on the current "recommended systems" list as approved by the JH Institutional Computing Standards Committee (ICSC)
         (1) Specific model selection will be determined in conjunction with the HSA IT Services LAN Administrator
   b) Desktops and laptops are typically replaced within the same fiscal year from when they reach 4 years of age from original purchase date
      i) Exceptions are handled on a case-by-case basis
   c) Dell Optiplex desktop computers running an approved version of the Microsoft Windows operating system are the recommended configuration for HSA staff
      i) Desktop computers are recommend because they are less prone to theft and potential data loss, are less costly to purchase and maintain, and typically have better performance then similar laptop configurations
      ii) Dell is the required vendor for all desktop computers managed by HSA IT Services
      iii) HSA IT Services will provide quotes for recommended system configurations and/or provide hardware from on-hand inventory
      iv) Personally Identifiable Information (PII) should not be stored locally on desktop computers
   d) Laptop computers may be requested if one or both of the following is true:
      i) Staff member travels regularly (> 25% of work time)
      ii) Staff member regularly works outside of their office (presentations, telecommutes, required for meeting use, etc. > 25% of work time)
         (1) Laptop approval is subject to review by the HSA Finance Operations office and staff member's Director or Dean

iii) Personally Identifiable Information (PII) should not be stored locally on laptops

e) Apple iMac Desktops and MacBook Pro laptops may be requested if:
   i) Staff member regularly uses applications that are optimized and/or only available for MacOS
      (1) Devices running MacOS may not be fully compatible with IT systems and applications, so consideration should be given to intended usage
      (2) MacOS device approval is subject to review by the HSA Finance Operations office and staff member's Director or Dean

2) Security
   a) Laptops
      i) Hardware must support full disk encryption
         (1) Must have a Trusted Platform Module (TPM) chip
         (2) Laptops will be encrypted by HSA IT Services prior to distribution to staff members
         (3) Encryption keys will be centrally stored in IT@JH-managed key storage repositories (MBAM, Airwatch)
      ii) Staff should strongly consider using a physical cable lock (Kensington, etc.) to secure laptops when not in use, especially during travel
      iii) When not in use, staff should log-out or lock screen (ctrl-alt-del) even if unattended for short periods of time that would not otherwise engage the auto-lock feature
   b) Tablets
      i) Procurement of tablets is normally funded through individual departmental budgets, not centrally
      ii) HSA IT Services approved tablets are:
         (1) Apple iPad (current models of Mini, Air, Pro)
         (2) Microsoft Surface (current models)
      iii) Tablets must be encrypted before use
         (1) Apple iPad: PIN must be enabled by user in Settings to activate encryption
         (2) Surface must be imaged/configured by HSA IT Services to activate encryption
         (3) For Outlook/Exchange email access, tablet must be configured for ActiveSync (or currently required device manager) in order to access Outlook/Exchange email.
         (4) "Find / Locate" services should be enabled by user to assist in locating lost or stolen devices
         (5) Screen lock time-out should be set to shortest time possible to enhance security
         (6) Personally Identifiable Information (PII) should not be stored locally on tablets
   c) Desktops
      i) Hardware must support full disk encryption
      ii) Must have a Trusted Platform Module (TPM) chip

iii) Desktops will be encrypted by HSA IT Services prior to distribution to staff members
iv) Encryption keys will be centrally stored in IT@JH-managed key storage repositories (MBAM, Airwatch)
v) When not in use, staff should log-out or lock screen (ctrl-alt-del) even if unattended for short periods of time that would not otherwise engage the auto-lock feature

3) Personally owned laptops and desktops (Bring Your Own Device)
   a) BYOD laptops and desktops not permitted for work-related use on campus
   b) May be used from home or off-campus for email (webmail) and remote desktop access via VPN
      (1) Personally Identifiable Information (PII) should not be stored on personally owned devices
   c) Other usage scenarios, including departmental Business Continuity Plans (BCP), should be discussed with a HSA IT Services LAN Administrator prior to implementation
4) Smartphones
   a) Both university-owned and personally-owned smartphones must be configured for ActiveSync with PIN (or currently required device manager) in order to access Outlook/Exchange email
   b) "Find / Locate" services should be enabled by user to assist in locating lost or stolen devices
   c) Screen lock time-out should be set to shortest time possible to enhance security
   d) Personally Identifiable Information (PII) should not be accessed nor stored locally on smartphones
5) New Hires
   a) Existing computer is normally repurposed if new staff member is replacing a previously filled position
   b) HSA IT Services should be notified at least one week in advance of start date so that the computer can be reconfigured for a new user and shared drives mapped, if requested.
      i) https://itservices.johnshopkins.edu/catalog/selfservice.do
   c) JHED ID will be needed before staff member can log into their computer
      i) https://my.jh.edu → First Time Login to activate new hire JHED ID
      ii) **Departmental Admin/Coordinator** should confirm Outlook/Exchange email account has been requested for new hire
   d) If new computer is required (new position), please submit online request form at: http://studentaffairs.jhu.edu/computing/help/computer-request-form/
6) Helpful links:

http://www.it.johnshopkins.edu/about/committees/icsc/

http://www.it.johnshopkins.edu/services/mobiledevices/mobility/activesyncsetup.html

Last Updated: February 2016