3014E Hardware Purchasing Policy

This policy corresponds to information also referenced in AHC-IS #3001E Desktop Support Policy. The intention of this policy is to:

1. Document purchasing services for those areas supported by AHC-IS
2. Ensure AHC computer hardware and software standards and license agreements are followed
3. Ensure all security measures are implemented prior to use of computer hardware
4. Ensure documentation exists for all warranty and return activities

Procedure

Please see new Policy #3038E for procedure on submitting Request for Purchase web form.

AHC-IS provides purchasing services for all supported customers / offices / areas. This service includes the following components:

- Standard desktop or laptop computer configurations for both Mac and PC will be available for an expedited delivery time. These configurations are designed to meet 80 – 85% of typical computer needs for tasks within the AHC.
- AHC-IS will also customize a computer configuration to meet specific needs. AHC-IS will assemble a proposal/quote of recommended hardware components along with associated costs for customer review prior to placing any custom order.
- Upon AHC-IS receiving approval from the customer/office/area, AHC-IS will place the necessary order(s) for hardware or software. The customer will be required to provide an appropriate EFS string for the order(s).
- All purchase orders are placed via EFS with approvals supported through an agreed upon process established between AHC-IS and the customer/office/area.
- All hardware orders is delivered to the AHC-IS computer set-up area (Minneapolis or St. Paul locations).
- The AHC Finance Cluster will process all payments of invoices.
- Pertinent information about the hardware and software is entered into AHC-IS desktop management database (ITASCA).
- AHC-IS will un-box hardware, install all necessary software, security profiles, and network configurations per University Private Highly Restricted data policy.
- AHC-IS will contact the customer to arrange additional software and/or data transfer.
- AHC-IS will then contact the customer/office/area to schedule time for installation.

AHC-IS Responsibilities

- AHC-IS will continually work with vendors to secure the best quality products at the lowest prices.
- AHC-IS will research new products as they are introduced to the market so configurations are continually updated and the customer receives up-to-date technology.
- AHC-IS will make every effort to minimize order and installation lead-time so customers receive new hardware and software ASAP.
- AHC-IS will stay current on evolving security threats and ensure all new equipment has the most current security patches, anti-virus software, and network configurations.
- AHC-IS will install only legally licensed software on the computers guaranteeing compliance with University license agreements.
Departmental Responsibilities to AHC-IS

- AHC-IS requires that supported customers/offices/areas do not independently order computer hardware or software. This process is the responsibility and a service provided by AHC-IS.
- If supported customers/offices/areas have inadvertently ordered and taken delivery of computer hardware or software, please submit a Computer Consultation & Support Request form. Those orders that were processed through AHC-IS according to this policy will have priority. If the equipment inadvertently ordered by the department does not meet AHC current standards, AHC-IS will not set up or install the equipment. AHC-IS will advise on a better option for compliance if the purchased equipment does not meet standards.
- No computer equipment should be connected to the University network in the Health Care Component without first being configured and secured. Violation of this point can introduce significant security risks not only to the immediate hardware, but to all equipment connected to the University network. (ref. UIS Policy)
- In order to meet compliance for the University any violations of UIS or Privacy policy within the AHC or units dealing with PHI or HIPAA related data will be relayed to the Security and Compliance groups.