Essential IT Policies

- Understand Data Classification at UT (Categories I, II and III data)
- Every computer must be encrypted including personal tablets and phones if used with UT data
    - exceptions may be granted by ISO on a case by case basis by using the form at https://forms.security.utexas.edu/misc/exception

- Every computer should be registered with a management console (Absolute Manage for Macs and SCCM (Software Center)) for PC's)
    - Windows PC's should be members of the Austin.utexas.edu domain
    - Adding Linux PC's to the Austin.utexas.edu domain reduces administrative overhead by limiting the number of local accounts to manage

- Tightly control administrative accounts
    - http://security.utexas.edu/policies/irusp.old

      5.4.7. **This section to be made effective on September 01, 2015 so as to allow the campus time to plan and transition.**

      Exception can be applied for when access to a university-owned IT device's administrative account is required by someone other than an IT Support Staff member, the following exception criteria must apply:

      5.4.7.1. Individuals must annually complete the Position of Special Trust form;

      5.4.7.2. Individuals must only use the administrative account for special administrative functions and default to a lower privileged user account for other day-to-day use;

      5.4.7.3. Individuals must review the following training materials, How not to Login as Administrator (and still get your job done);

      5.4.7.4. IT System Custodians are required to periodically review the use of administrative account exceptions.

      5.4.7.4.1. IT System Custodians will remove any administrative accounts that go unused or are no longer required; and

      5.4.7.4.2. IT System Custodians are required to raise inappropriate use to management (e.g., staying logged in with the administrative account longer than needed).
- Procurement
    - All units are required to have their local IT Systems Custodian(s) participate in processing (e.g., inventory, standards verification, configuration) of all IT procurements
      (e.g., network-capable computing devices and large dollar or high risk software). This includes but is not limited to any university owned devices that have the ability to
      store university data or use the university wired or wireless networks. Examples of these types of computing devices include but are not limited to: laptops,
      desktop computers, tablet devices, and servers.
- TBD policy spot checks for UT owned computing equipment. Monthly?