Technology Acquisition Lifecycle Management High Level Process

Parent Policy: Technology Acquisition Lifecycle Management

Associated High Level Processes: Computer Refresh, and Computer Retirement

Contents

1. Scope and Purpose .......................................................... 1
2. Process and Procedure ..................................................... 1
   2.1 Plan and Acquire Phase ................................................. 2
   2.2 Configure and Deploy Phase ......................................... 4
   2.3 Maintain, Support, and Upgrade Phase ......................... 5
   2.4 Decommission, Retire, and Dispose Phase ...................... 6
3. Applicable Roles, Responsibilities, and Skills ....................... 7
4. Measurement and Metrics .................................................. 8
5. Continual Improvement ..................................................... 8
6. Resources ............................................................................. 8

1. Scope and Purpose
This high level process supports the implementation of the Technology Acquisition Lifecycle Management Policy. The policy applies to all University (USF) information technology assets, resources, services, and Users in all locations. (See the glossary (in the knowledge base) for the definition of terms used in this document).

2. Process and Procedure
1. ITS will implement reasonable security practices and procedures to safeguard the asset aligned to authoritative information security standard frameworks and controls, (e.g. ISO, NIST, PCI, SANS-CIS, etc.) to comply with Federal, State, and local laws and regulations. ITS will work in conjunction with designated information stewards, asset owners, Schools, Colleges, and Departments, to implement the safeguards using a risk-based approach. The higher the value of the asset or the more it is viewed to be at risk, the higher level of protections will be employed. These will be applied across each phase of an assets lifecycle:

   - plan and acquire,
   - configure and deploy,
   - maintain, support and upgrade,
   - decommission, retire, and dispose.

2. Each phase of the lifecycle must include the involvement of the Vice President - Chief Information Officer (VP-CIO), or delegate, to ensure the asset conforms to standards related to technology, architecture, security, data classification, service delivery, service operation,
disposal, and license management. The VP-CIO will ensure all assets conform to the standards and procurement policy irrespective of funding source\(^1\).

See FAQ/How Do I? on the procedure to involve the VP-CIO. This includes defining what "involvement" means as far as concurrence to move forward, adherence to standards, and addressing any exceptions.

The following process requirements apply to all three asset categories - infrastructure, applications, and endpoints - unless otherwise indicated as being category specific. (The italicized text indicates the active response that USF ITS utilizes to satisfy the requirements. The internal Standard Operating Procedures (SOP) are ITS access only.)

### 2.1 Plan and Acquire Phase

Planned acquisition of new hardware, software, application, and services assets must be done in conjunction with ITS to ensure the assets conform to the University's technology standards, procurement process, and are integrated and supported effectively to maximize the assets value.

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Applications</th>
<th>Endpoint Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. This phase includes plans to acquire network devices, LAN printers, servers for applications, databases and infrastructure services, and all network and system management tools.</td>
<td>1. This phase includes plans to acquire multi-user or enterprise-class applications (and databases) for use by one or more Departments or Faculties. The applications and databases may be for installation in the University data center, or be acquired as a service (Software as a Service, SaaS) from an external provider.</td>
<td>1. This phase includes plans to acquire University purchased Personal Computers (PCs) running Windows or Apple OS, or iOS (iPad tablets), and associated personal productivity software installed on the PC as part of the standard &quot;image&quot;.</td>
</tr>
<tr>
<td>See FAQ/How Do I? involve ITS in acquisitions not initiated by, or not initially involving ITS.</td>
<td>See ITS in acquisitions not initiated by, or not initially involving ITS. See FAQ/How Do I? get an external service or SaaS, assessed by ITS? This</td>
<td>See Computer Refresh HLP.</td>
</tr>
<tr>
<td>**(^1)**Hardware and software purchases must follow ITS technical standards and conform to the security standards(^2). ITS follow an internal SOP to maintain the technical standards.</td>
<td>2. Applications must be assessed for their ability to integrate into the current IT system and security safeguards. See How do I? get an external service or SaaS, assessed by ITS? This</td>
<td>2. PC hardware and software purchases must follow ITS technical standards. See Hardware Standards and Software Standards. See Computer Refresh HLP for procedures to request new hardware and</td>
</tr>
</tbody>
</table>

\(^1\) Includes assets bought under ITS budget, under the centrally funded the Computer Refresh (CR) Program, by individual units, and by grant and special account funding.

\(^2\) See Information Security High Level Process (HLP) for details of "reasonable security procedures and practices".
standards. includes: (i) integrating applications into the University's identity access management and authorization system to enable User's "single sign on" (SSO) from their USF username.
(ii) conformance to the network and infrastructure standards and security standards, and (iii) conformance to the information classification scheme and information management protections particularly if data is hosted externally.

ITS follow an internal SOP to assess internal and external application compliance to security and technical standards.

### 3. Where possible, infrastructure assets must be purchased from the University’s preferred vendors to ensure the University achieves maximum discounts, and to comply with purchasing policy.

### 3. Endpoint assets must be purchased from the University’s preferred vendors to ensure the University achieves maximum discounts, and to comply with purchasing policy. An exception policy exists. See Computer Refresh HLP.

### 4. Purchases of tablet computers must be procured centrally through ITS and funded by local departments (via grant or special account funding) from preferred vendors. See Computer Refresh HLP.

---

3 See Information Security High Level Process (HLP) for details of "reasonable security procedures and practices".
5. Purchases from non-preferred vendors must be done using the standard hardware exception request process, and receive both ITS and local departmental budget approval. Only employees can buy tablets. See Computer Refresh HLP.

6. Tablets with cellular capability must adhere to the reimbursement policy described in the Accounting and Business Service (ABS) electronic communications policy.

### 2.2 Configure and Deploy Phase
Several tasks and work are required to ready the asset for service and ensure secure operations.

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Applications</th>
<th>Endpoint Assets</th>
</tr>
</thead>
</table>
| 1. All assets must be inventoried and physically asset tagged by ITS.  
*ITS follow an internal SOP to ensure new assets are tagged and added to the asset inventories.* | 1. All assets must be inventoried by ITS.  
*ITS follow an internal SOP to ensure new assets are added to the asset inventories.* | 1. All assets must be inventoried and physically asset tagged by ITS.  
*ITS follow an internal SOP to ensure new assets are tagged and added to the asset inventories.* |
| 2. It is the responsibility of the employee to notify ITS when a PC or tablet is reassigned to another member of the University, or when the PC or tablet has failed, gone missing, or reached the end of its useful life cycle. See Computer Refresh HLP. |  | |
| 3. All assets must be configured to satisfy the University’s security standards. If this is not possible an exception must be filed before deployment. This is subject to approval. As part of the exception request there must be an alternative security mitigation put in place prior to asset setup. |  | |

---

4 See top level KB site that has detailed procedures for configuring assets.
being moved into production that provides an acceptable level of security. See Exception Process for more.

*ITS follows an internal SOP to record that assets are classified and configured so that reasonable security controls are present, or if missing, that they will be established. If standard controls missing then approved non-standard mitigations must be added with ITS approval, and the risk status of the asset agreed with the Information Steward updated in the inventory.*

| 4. | All assets must have an Information Steward assigned. This extends to ITS owned and managed systems and software and contracted systems and services outside of the University. |

*ITS follows an internal SOP to identify and maintain an up-to-date inventory of the Information Stewards.*

| 4. | Each PC and tablet asset must have a designated Asset Responsibility Owner (ARO). An asset may have Primary Client if used by non-employees. |

*ITS follows an internal SOP to keep and maintain an up-to-date inventory of PC and tablet assets.*

| 5. | All assets must have a support plan, an internal Operating Level Agreement (OLA), or Service Level Agreement (SLA) in place prior to being moved into production. The support plan must include a disaster recovery plan. This FAQ describes what is in an asset disaster recovery (DR) plan and the steps to develop one. |

*ITS follows an internal SOP to identify, develop, and maintain an up-to-date DR plan for each major asset and associated OLA or SLA.*

| 5. | All assets must have a support plan in place and a Service Level Agreement (SLA) prior to being moved into production. The support plan must include a disaster recovery plan for the asset. This FAQ describes what is in a disaster recovery (DR) plan for the asset and the steps to develop one. |

*ITS follows an internal SOP to identify, develop, and maintain an up-to-date DR plan for each major asset and its associated SLA.*

| 6. | See [ITS Support Priority Guidelines](#) |

### 2.3 Maintain, Support, and Upgrade Phase

Assets must be maintained and supported over their useful life to ensure they continue to operate safely and securely. This extends to any upgrades, significant or otherwise, that an asset may undergo.

---

Classification | Internal
Page 5 of 8
Infrastructure | Applications | Endpoint Assets
---|---|---
1. Assets must operate according to ITS operating procedures and standards which includes inventory management, patch management, change management, access management, security, backup, incident management, and disaster recovery. Assets must not be exchanged or traded without approval from the VP-CIO. How Do I? request approval from the VP-CIO?

*ITS follows an internal SOP to operate assets according to the ITS operating procedures and standards.*

2. Agreed and required levels of service, and details of support and availability, must be documented in a Service Level Agreement (SLA). External applications and services should include details on their level of conformance to ITS standards and any required exceptions. See library of SLAs for assets and filed exceptions.

*ITS follows an internal SOP to track and manage SLAs and the level of conformance to ITS operating procedures and standards.*

3. Upgrades to assets must be done as a project, i.e. following an approval process, and including assessments for conformance to standards for security, infrastructure, application, data architecture, and technical architecture.

*ITS follows an internal SOP to manage upgrades and replacements of information assets.*

### 2.4 Decommission, Retire, and Dispose Phase
Assets must be securely and appropriately decommissioned and disposed of at the end of their design or useful life. This extends to any replacements.

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Applications</th>
<th>Endpoint Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Retirement and decommissioning of infrastructure assets must be done in a manner that it does not compromise the confidentiality, integrity, and availability of the data and information. ITS must work closely with the asset’s Information Steward. Network devices, LAN printers, and servers must be wiped of any network configuration settings, and data in memory, on disks.</td>
<td>1. Retirement and decommissioning of applications must be done in a manner that it does not compromise the confidentiality and integrity of the data and information. ITS must work closely with the asset’s Information Steward to either transition information to a new application, archive the information if required by the retention schedule, or ensure its destruction.</td>
<td>1. PCs must be retired and disposed of following the Computer Retirement HLP. This includes all centrally purchased PC replaced under the Computer Refresh (CR) Program, and PC and tablets purchased under departmental, grant, or special funding.</td>
</tr>
</tbody>
</table>

*ITS follows an internal SOP to securely decommission and retire information assets.*

---

5 See top level KB site that has detailed procedures used to maintain, support, and upgrade assets.
3. Applicable Roles, Responsibilities, and Skills
For more expanded details see the Roles & Responsibility document.

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
<th>Skills/Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO</td>
<td>Provide guidance to other roles.</td>
<td>Security policy and practices.</td>
</tr>
<tr>
<td>Asset Responsibility Owner</td>
<td>Inventory and know the list of hardware assets under their control. Assess the assets for risk, and set degree of tolerance. Approve who has authorized access or not. Assess asset life cycle for replacement / retirement.</td>
<td>Know assets under their control. Know access lists. Know replace/retire decision.</td>
</tr>
<tr>
<td>Information steward</td>
<td>Inventory and maintain the list of data, information, and application assets under their control. Classify information on the asset. Assess the assets for risk and degree of tolerance. Assess and as necessary approve who has authorized access to information.</td>
<td>Must know what assets support the business processes under their control, and who needs access and to do what. Must have knowledge of how to apply information classification scheme.</td>
</tr>
<tr>
<td>Users</td>
<td>Maintain the confidentiality, integrity and availability (CIA) of the assets they access, use and interact with.</td>
<td>Must know how to maintain the CIA of the assets. Must know what threats could expose the assets they access, use and interact with and what they can do to protect against these.</td>
</tr>
</tbody>
</table>

6 See top level KB site that has detailed procedures to decommission, re-purpose, and dispose assets.
### ITS Technical Staff

| Acquire and deploy reasonable security practices (safeguarding policies, standards, controls and procedures) based on risk assessment from Information Steward to safeguard the security of the assets. Check for compliance to centrally-managed client software agreements. | Must implement reasonable security practices and provide documented assurance that they are operating as designed and intended. |

---

### 4. Measurement and Metrics

1. **Lagging results indicators:**
   - number of assets found to have been acquired or disposed of without following Policy or this process.

2. **Leading results indicators:**
   - number of assets following this process,
   - number of assets repurposed and disposed of,
   - number of "single license" software purchases versus "site license" volume agreements,
   - number of licenses re-used under centrally-managed client software agreements (e.g. report on number of Microsoft Office licenses currently installed),
   - reduction in audit time due to up to date inventory of assets.

### 5. Continual Improvement

This process will be reviewed in conjunction with the review of the Technology Acquisition Lifecycle Management Policy.

### 6. Resources

- [Technology Acquisition Lifecycle Management Policy](#)
- [Computer Refresh High Level Process](#)
- [Computer Retirement High Level Process](#)
- [Information Security High Level Process](#)
- [Information Classification standards](#)
- [Roles and Responsibilities](#)
- Information Access standards
  - [Standards and Glossary](#) - use the [Knowledge Base](#) for security standards, technical controls, and glossary terms.
  - [ServiceNow ITS knowledge base and procedures library](#) - use Search box to find a specific guide or article.
- [ITS Help Desk](#) - use for general IT assistance.
- [Exception Process](#) - use to request an exception related to this process.