Computer Retirement Policy

<table>
<thead>
<tr>
<th>Policy Contents</th>
<th>Effective Date: 03-01-2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. POLICY STATEMENT</td>
<td>Last Updated: 02-18-2015</td>
</tr>
<tr>
<td>II. REASON FOR POLICY</td>
<td>Responsible University Officer:</td>
</tr>
<tr>
<td>III. SCOPE</td>
<td>Opinder Bawa</td>
</tr>
<tr>
<td>IV. AUDIENCE</td>
<td>Vice President, Chief Information Officer</td>
</tr>
<tr>
<td>V. POLICY TEXT</td>
<td>Policy Owner:</td>
</tr>
<tr>
<td>VI. PROCEDURES</td>
<td>Director, Client Support Services</td>
</tr>
<tr>
<td>VII. RELATED INFORMATION</td>
<td>Policy Contact:</td>
</tr>
<tr>
<td>VIII. DEFINITIONS</td>
<td>ITS Help Desk</td>
</tr>
<tr>
<td>IX. FREQUENTLY ASKED QUESTIONS</td>
<td></td>
</tr>
<tr>
<td>X. REVISION HISTORY</td>
<td></td>
</tr>
<tr>
<td>XI. COMPLIANCE</td>
<td></td>
</tr>
<tr>
<td>XII. POLICY EXCEPTION PROCESS</td>
<td></td>
</tr>
<tr>
<td>XIII. APPENDICIES</td>
<td></td>
</tr>
</tbody>
</table>
I. POLICY STATEMENT
   A. All retired USF-owned computers will be returned to ITS and inventoried and after 10 days the data stored on the computer will be destroyed. After the data on the retired computer has been destroyed, the retired computer can be donated or sold. If sold to a third-party vendor, the vendor must wipe the hard drive clean and provide a certification of data destruction to ITS. Computer retirement shall comply with applicable laws, regulations, and software licensing.

II. REASON FOR POLICY
   A. The purpose of this policy to create an authorized process for retirement of computers purchased through USF's Computer Refresh Program (RP) that complies with applicable laws, regulations, and software licensing.

III. SCOPE
   A. This policy covers all USF-owned computers that were purchased through USF’s Computer Refresh Program.

IV. AUDIENCE
   A. This policy is intended for all USF faculty and staff who use USF-owned computers that will one day be retired in accordance with this policy.

V. POLICY TEXT
   A. Objectives
      1. Efficient use of University resources: The policy is designed to minimize University computer pick-up costs, including labor and transportation.
      2. Maximum sell-back cost recovery and timely delivery to donation recipients: The policy is designed to reduce unnecessary equipment aging, which reduces sell-back value, as well as ensure that retired computers are available to mission-related projects in accordance with expected time frames.
      3. Compliance with applicable laws: Laws such as Gramm-Leach-Bliley Act (GLBA), FERPA (Family Educational Rights and Privacy Act) and HIPAA (Health Insurance Portability and Accountability Act) require that the University safeguard confidential information which may be stored on desktop and laptop computers. This requires that all retired computers be re-inventoried and de-provisioned by ITS.
4. Compliance with EPA (Environmental Protection Agency) regulations: The University must ensure that all computers are responsibly disposed.
5. Compliance with Software Licensing Policies: The University must ensure that all licensed software is removed from retired computers in accordance with current licensing agreements.

B. Computer Retirement Policy
1. All computers due for refresh during the Computer Refresh Program year must be scheduled for refresh from February 1st - November 30th.
2. Computer systems ordered by a Division or College's Refresh Program Coordinator cannot be changed or exchanged for a different Refresh Computer.
3. All university computers purchased through the Refresh Program must be collected on the day that the replacement computer is installed.
4. All retired computers will be inventoried in the ITS Inventory Facility. All computers stored in ITS will be encrypted until donated or resold. Retired computers will be stored in ITS for 10 business days. During the 10 business days, former users of the computer may contact ITS to recover any missing data from their old computer. However, after 10 business days, all data stored on the hard drives will be destroyed using a Department of Defense (DOD) 5220-22.M Standard 7-Pass Wipe.
5. Retired computers resold to third-party vendors will be wiped for a 2nd time using a DOD 5220-22.M Standard 7-Pass Wipe. All vendors are required to provide ITS a certification of data destruction.
6. Computer equipment from separated faculty and staff members must be collected by the supervisor. The supervisor must review the data contained on the hard drive with an ITS technician and place any files requiring continued use on the central ITS file server. After reviewing the contents of the hard drive, the computer will be wiped and re-inventoried or assigned to a replacement hire.
7. Computing equipment for the separated employee must be received from the supervisor within 10 business days of separation. Local departments must pay for the cost of any devices not returned to ITS.

VI. PROCEDURES
A. All University Faculty and Staff members who have a USF computer scheduled for replacement are contacted by their division or college's RP Coordinator by February of the replacement year, which provides Faculty and Staff 6 months to schedule an appointment for replacement.
B. The Faculty or Staff member contacts ITS to schedule the refresh (i.e., they will receive a newer replacement computer).
C. On the same day that a replacement computer is installed, the retired computer is collected by ITS.
D. During the first 10 days, the user can contact ITS to recover any missing data from their old computer.
E. After 10 days, the data stored on the hard drives of the old computer will be destroyed using a Department of Defense (DOD) 5220-22.M Standard 7-Pass Wipe.
F. If the retired computer is sold to a third-party vendor, the vendor performs another DOD 5220-22.M Standard 7-Pass Wipe and sends ITS a certificate of data destruction.

VII. RELATED INFORMATION
A. (None)

VIII. DEFINITIONS
A. Replacement Program
   1. University of San Francisco's annual technology program that replaces University-owned computers that have reached the end of their useful life. This program has a central budget.
B. Computer Retirement
   1. After a University-owned computer reaches the end of its useful life, the computer must be properly removed from campus network and all data contained on the hard drive must be destroyed (wiped).
C. Disk Wiping
   1. The process of securely erasing data from a computer's hard drive by writing random data multiples times over the sectors of hard drive. USF ITS uses a Department of Defense (DOD) 7-pass wipe (writes random data 7 times).
D. UITC
   1. University Information Technology Committee
E. Desktop Computing Subcommittee
   1. USF's IT Governance subcommittee that oversees the maintenance and development of USF's desktop computing environment.
F. FERPA
   1. The Family Educational Rights and Privacy Act of 1974, commonly referred to as the Buckley Amendment, protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.
G. GLBA

H. HIPAA
1. Health Insurance Portability and Accountability Act is a federal regulation establishing national standards for health care information.

I. Software Piracy
1. Unauthorized copying or installation of software

IX. FREQUENTLY ASKED QUESTIONS
A. (None)

X. REVISION HISTORY
A. 04-22-2014 – First publication
B. 03-01-2015 – Updated to new format and minor edits

XI. COMPLIANCE
A. Failure to follow this policy can result in disciplinary action in accordance with Human Resources Employment Handbook and Office of General Counsel employee and labor relations. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

XII. POLICY EXCEPTION PROCESS
A. A proposed exception request to ITS Policy requires a formal e-mail explanation related and in support of job function.
B. A proposed exception request to ITS Policy, mentioned in 'XII.A', must be approved via email by respective department or division supervisor, Dean, or VP, before submitted to ITS for review.
C. Forward approved email as stated in 'XII.B' to itshelp@usfca.edu for processing.
D. Evaluation of ITS Policy Exception will escalate internally, and as applicable may include further review by: UITC subcommittee(s), the Information Security Officer, and others as appropriate at the request of VP for IT.

XIII. APPENDICIES
A. (None)