Issue Date:
 2004-03-10

 Last Updated:
 2017-12-17

 Updated By:
 Lisa Mildon

 Revision:
 1.3

# INFORMATION TECHNOLOGY

# ENDPOINT MANAGEMENT MANUAL

# **Table of Contents**

Introduction	page 3
Endpoint Management Standards	page 4
New PC Deployment Protocol	page 6
Upgrade a Computer by use of PXE	page 7
Windows 7 Endpoint Checklist	page 14
Naming Convention	page 15
Install McAfee Endpoint Encryption	page 16
Inventory Updating Procedure	page 24
CS Inventory Surplus Procedure	page 26
Tripwire Procedure	page 28

#### Introduction

The following document details the processes and procedures followed by Tulsa IT staff in managing university-owned endpoints. This manual should enable IT staff to manage and configure an endpoint from the time it arrives on campus to the time it is removed from production and disposed. Included in the manual are the baseline standards for endpoints being placed on the OU-Tulsa network. Additionally, technical instructions and inventory management procedures are included for use by Tulsa IT staff. All Tulsa IT staff should conform to and abide by the information and instructions contained in this manual. Each procedure found in the manual is available on the OU-Tulsa IT team collaboration site <a href="https://share.ou.edu/sites/IT/tulsa/CS/default.aspx">https://share.ou.edu/sites/IT/tulsa/CS/default.aspx</a>. The information contained here will be reviewed annually and updates will be made as they are needed.

### **Endpoint Management Standards**

The following controls are required for all endpoints deployed at OU-Tulsa and placed on the network:

- Client Management
  - Active Directory
    - Member of the university active directory
    - Subjected to all university global group policies (GPO)
    - Follows standard naming convention. (See page 15.)
    - o Antivirus
      - Member of the university anti-virus solution (McAfee Antivirus)
      - Configured to provide automatic virus definition updates on at least a daily basis
      - Configured to provide centralized alerting and reporting of malware infections
    - Patch management
      - Member of OU-Tulsa patch management process
      - Enforce at least monthly patching of critical security vulnerabilities, which includes Microsoft updates
      - McAfee Antivirus will be updated automatically as updates are released
      - Palo Alto transmits patches as they are developed by company support team
    - o Vulnerability management
      - Member of a university vulnerability scanning group (Tripwire)
      - Vulnerability scanning performed once monthly
      - IT staff will review reports and remediate all vulnerabilities based on the following schedule:

Vulnerability Rating	Time
Medium	1 month
High	1 week
Critical	ASAP

- o Inventory Management
  - All Endpoints must have an entry in the Service Now inventory
  - Records must meet minimum standard set by IT: see page 23
- Client Configuration
  - o Secure baseline
    - Client must run a university- and vendor-supported operating system
    - Client configuration based on Microsoft baselines (preferably configured via GPO)
    - IT will create and utilize system images with built-in baseline configurations
    - Mobile devices (laptops) must be encrypted utilizing university approved encryption software (McAfee Endpoint Encryption): see page 16

- o Accounts
  - Users of endpoints will be granted local administration rights based on user's role. Faculty, Administrative staff, and laptop owners will be granted administration rights with the exception of residents
  - The domain administrators group must be a member of the local administrators group
  - The OUHSC\TULSA-DesktopAdmins account must be a part of the local administrators group. OUHSC\Tulsa-MedInfo Admins will be a part of the local administrators group on all clinical endpoints
- o Logging
  - Local event logging enabled
    - Logging levels—system events
- o Other
  - Customer must not install or use software of the following types:
    - o P2P file sharing applications. See: <u>http://it.ouhsc.edu/policies/Peer-to-peer.asp</u>
  - The following security measures will apply to each endpoint:
    - Compromised or malware infected systems will have their network connections disabled immediately to prevent spread of infection or exfiltration of data
    - o Sensitive university data should not be stored locally to the desktop hard drive
    - o Endpoints must not access third party mail providers

Additional Requirements to be placed on HSCACCESS wireless Network:

• Device must be encrypted

0

- Laptops and tablets with a full OS with must have full disk encryption
- Mobile devices will utilize Secure Mobile via email app
- Device must have an inventory record in ServiceNow
- o Device must be whitelisted in InfoBlox
- Laptops and tablets with a full OS should have:
  - McAfee Agent
  - McAfee Antivirus (PC) or Endpoint Security (Mac)
  - GlobalProtect Client

# **New PC Deployment Protocol**

**<u>Purpose:</u>** To provide required steps and processes needed for the deployment of new computers.

**Scope:** This document covers the steps and processes related to Client Services configuration and deployment of new computers.

#### **Definitions:**

CS – Client Services

#### Procedure:

- 1. Upon arrival of order, work order becomes available for building, configuration and deployment
- 2. CS technician checks work order for any specific instructions.
- 3. Create computer account in AD (Tulsa or Sooner).
  - a. Must use the following naming convention:
    - i. For OUHSC PC's: OUT-dept-username (or may be location, something unique)
    - ii. For College of Education PC's: EDUC-location
    - iii. For Arts and Sciences
    - iv. Tulsa Grad College TGC- location
    - b. In the description line, enter the model, service tag\serial number and warranty expiration date.
- 4. Image PC with image off PXE (\\out-wds\REMINST\Images)
- 5. Change name of PC to match the new name in AD.
- 6. Put PC on domain.
- 7. Apply any Microsoft, McAfee or anti-spyware updates.
- 8. If PC is a laptop then encrypt laptop with McAfee Endpoint Encryption
- 9. Contact purchaser and\or end-user to get any specific installation instructions.
  - a. Special software.
    - i. New license or transfer of license.
  - b. Printers installed.
  - c. Other hardware.
  - d. New or existing user.
    - i. If existing user, either notify them to backup personal files or offer assistance.
  - e. What date\time would be best for installation?
- 10. Input Inventory information into Service Now (see p. 23 Inventory Updating Procedure)

**Enforcement:** Failure to comply will be met with appropriate disciplinary action as determined by the OU standards for Positive Discipline included in *The University of Oklahoma Staff Handbook* 

# Upgrade a Computer by Use of PXE

#### 1.0 Purpose

This document sets out to provide the steps needed to (re)image a computer to run Windows 7 via the use of PXE over the OU-Tulsa network

#### 2.0 Scope

This document applies to any computer (desktop and laptop) owned by or operated by OU-Tulsa, associated departments, clinics, off-site clinics and affiliates that connect to the OU-Tulsa network

#### 3.1 Policy

- 3.2 Steps for PC and Laptop
  - 1. Log into PC and
    - a. Record PC Name
    - b. Record printers installed
    - c. Record non-standard software installed
    - d. Back-up user files in the following folders Desktop, My Documents, Favorites
    - e. Back-up Outlook .pst files (if Outlook is setup and in use)
      - i. Reboot PC
  - 2. On system boot, insure the NIC is bootable (image 1)
    - a. Press F12 to bring up boot options.
      - i. Go to System Config
      - ii. Integrated NIC
      - iii. Enable with PXE
      - iv. Press Apply and then Exit

Settings Ceneral Date Time Boot Sequence System Configuration USB Consider - USB Consider - Parallel Port	Integrated NIC
Parallel Port Address     Social Port #1     Miscellameoras Devices     Video     Performance     Viduo     Socialty     Power Management     Mainteenance     MagabServer     Post Behavior     System Logs	This field enables and disables the integrated Network Interface Controller (NIC). Disable = Integrated NIC is disabled Enable = Integrated NIC is called Enable with RXE = Integrated NIC is on (with RAE enabled) Enable with ImageServer = Integrated NIC is on (with ImageServer enabled) Note: ImageServer is incompabile with RAE mode. Please disable RAD if enabling ImageServer. Note: RXE is needed only if intending to boot to an operating system located on a server, not if you are booting to an OS located on a hard drive in this system.
	Load Defaults Eas

(image 1)

- 3. For older system SATA operation will need to be set.
  - a. Under Drives-SATA Operation, select AHCI.
- 4. Press F12 to bring up boot options (image 2)a. Select Onboard Network Controller

 Issue Date:
 2009-10-06

 Last Updated:
 2016-06-15

 Updated By:
 Lisa Mildon

 Revision:
 2.1

- b. Press Enter
- c. Press F12 when prompted

```
Onboard or USB Floppy Drive
ST316001585
Onboard or USB CD-RDM Drive
Onboard Network Controller
System Setup
Diagnostics
Intel(R) Management Engine BIOS Extension (MEBx)

Use Up/Down arrows to highlight desired item.
Use Enter to select highlighted item.
Intel(R) Boot Agent CE v1.3.22
Copyright (C) 1997-2008, Intel Corporation
CLIENT MAC ADDR: 00 22 19 26 48 ED CUID: 44454C4C 5200 1030 8046 C7C04F4D4A31
CLIENT IP: 10.130.154.21 MASK: 255.255.255.0 DHCP IP: 10.130.2.10
GATEWAY IP: 10.130.154.1
Downloaded WDSNBP...
Press F12 for network service boot
```

(image 2)

- 5. Select "Server 2008 & Windows 7 64bit setup" (image 3)
  - a. Press Enter



(image 3)

6. Leave as default and press Next (image 4)



2009-10-06 2016-06-15 Lisa Mildon

2 Install Windows	
Windows Deployment Services	
Locale: [English (United States) Keyboard or input method: [US	
	-
Copyright © 2009 Microsoft Corporation. All rights reserved.	Next
	Lie

(image 4)

7. Log in with your OUHSC A (admin) account (image 5)

	Connect to OUT-IT-P2	@.hvc.net.ou.edu	1×1	
	44			
	Enter your user name ir user@domain.com.	n the format domain/user or		
Keyboard o	User name: Password:	0		2
		ок	ancel	
Copyright @ 2009 Microso	t Corporation. All rights reser	rved.		Next

- 8. Select the appropriate image from the list. In this example it was "Windows 7 Project v5" (image 6)
  - a. Press Next

Issue Date: Last Updated: Updated By: Revision:

Tana and a second se				
Operating system	Language	Architecture	Date modelied	121
Peds v2	en-US	x64	1/25/2014	
Perinatal V2	en-US	x64	1/27/2014	
Windows 7 64 Bit, Office 2010 64 bit	en-US	x64	11/1/2013	
Windows 7 64 Bit, Office 32 Bit, Adobe Re	en-US	x64	11/5/2013	100
Windows 7 Project - v3	en-US	x64	12/12/2013	
Windows 7 Project - v4	en-US	x64	1/21/2014	
Windows 7 Project - v5	en-US	×64	2/14/2014	
Windows 7 Project - v5	en-US	364	2/14/2014	
Womens Clinic v1	en-US	x64	2/1/2014	*
Select (anguage to inital):				
				Next

(image 6)

- 9. Delete any existing partitions until only unallocated space remains (images 7 & 8)
  - a. Press Next

Name		Total Size	Free Space Typ	pe
Disk 0 I	artition 1: System Reserved	100.0 MB	71.0 MB Sys	stem
Disk 0 8	artition 2	148.9 GB	116.9 GB Pri	mary
Coad Driver	3 estado			

(image 7)

Issue Date:200Last Updated:201Updated By:LisaRevision:2.1

Disk 0 Unallocated Space 149.0 GB 149.0 GB	Name		Total Size	Free Space Type	
	Disk 0 Unall	ocated Space	149.0 G8	149.0 G8	
Befresh      Const      Now	€2-Befresh	Relete	Eormet	<b>#</b> Ngw	

(image 8)

10. "Installing Windows" will now run. Once completed the PC will auto reboot (image 9)

Installing Windows	
That's all the information we need right now. Your computer will restart several times during installation.	
Copying Windows files Expanding Windows files (0%) Installing features Installing driven Completing installation	
	De

(image 9)

- 11. "Finish Setup/Driver Install" will run on reboot and once completed the PC will auto reboot again
- 12. Name the computer (image 10)
  - a. Click the Next button
  - b. Select Restart Later (restart after joining PC to the domain)

Issue Date: Last Updated: Updated By: Revision: 2009-10-06 2016-06-15 Lisa Mildon 2.1



(image 10)

- 13. From another PC, create a new computer account in the Tulsa AD
  - a. Add PC to "tulsa.net.ou.edu" (remember to remove HSC AD account) (image 11)
  - b. Reboot



## (image 11)

- 14. Install McAfee ePO Agent from the following location/file
  - a. \\out-file\public\McAfeeAgent\ePO\_Agent\_4. 8. 0. 1995.exe
  - b. Run "all" Windows Updates
  - c. Finish required software installs/setup
  - d. Copy backed-up User files folder to root of C:\
    - i. These can be returned to correct location once the user account has been created after they login for the first time
  - e. Add user as a Local Admin if appropriate to role
  - f. If a laptop, Setup Wi-Fi to use OUBASE
  - g. Modify the ServiceNow entry for the PC/Laptop or create a new entry

- 3.1 Additional steps for encrypted Laptops
  - 1. Log into encrypted pre-boot environment
    - a. If your account is not recognized, check with Lisa Mildon or Ben Tuttle
  - 2. Boot laptop and follow ALL steps in 3.1 above, then add the following final steps
    - a. Encrypt laptop (re-imaging "removed" encryption)
    - b. Add user to the computer in McAfee ePO
    - c. Check that user name is recognized by the encryption logon

4.0 Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action within the appropriate existing University employment guideline

# Issue Date: 2003-12-01 Last Updated: 2015-06-26 Updated By: Lisa Mildon Revision: 3.0

# Windows 7 Endpoint Checklist

	Username: PC Name:
	Department:
	Location: Service Tag#:
	Phone:
Needs / Dor	
<del>X</del>	Image computer using PXE
X	Create computer account in AD + Model, Service Tag # and warranty expiration date in the description.
<u>×</u>	Add to Domain (Name PC, add to Tulsa domain)
<u>x</u>	Update group policies (gpudate /force)
<u>x</u>	Update BIOS as needed
<u>x</u>	Update ePo Agent if needed
<u>x</u>	Update McAfee AntiVirus
<u>x</u>	Check Device Manager and update drivers from support.dell.com
<u>x</u>	Microsoft Updates from Windows update (Control Panel)
<u>x</u>	Change Folder properties to show full path in address bar and don't hide extensions PU Admin
<u>x</u>	Set Power to Never Sleep
<u>x</u>	Remove ability for Windows to turn off NIC power (Wireless and Hardline)
<u>x</u>	Update Java
<u>x</u>	Update Flash
<u>x</u>	Update Acrobat Reader
x	Install Printers:
	Update Citrix Receiver if needed
	Wireless devices
	Disable ad hoc wireless moderestrict to infrastructure only
	Configure wireless Ethernet connection to disable when computer is attached to wired network
	Disable Bluetooth collaboration (if applicable)
<u>x</u>	Encrypt, if laptop
	Inventory
<u>×                                    </u>	Input new install or transfer of PC into ServiceNow inventory
~	End user setup
<u>*</u>	Set Default Drister
<u>×</u>	Set Default Printer
<u>×                                    </u>	Map S & and any other network No backup.
<u>×                                    </u>	Kestore user's backup
	Additional Software

# NAMING CONVENTION

abbrev.	Dept
CC	CallCenter
CAD	BedlamDept
ADM	AdminDept
CAD	CliAffDept
CB	CenBilDept
CAN	ChildAbuseNetwork
COM	DeansDept
PPC	DistanceED
EM	EmergencyDept
FMC	FamMedClinic
FMD	FamMedDept
HR	HumResDept
PACT	ImpactDept
IMC	IntMedClinic
IIC	IntegratedImmunologyCenter
IMD	IntMedDept
LIB	LibraDept
LC	LearningCenter
MI	MedicalInformatics
MRD	MedicalRecordsDept
NEU	NeurologyDept
OBD	OBDept
OPS	OperaDept
PC	PedsClinic
PD	PedsDept
PDC	PedsDiabDept
PSC	PsychClinic
PSD	PsychDept
RAM	Ramona
RSA	ResStuAff
SA	StudentAff
SC	SurgClinic
SD	SurgDept
SEC	SecurDept
STU	StuSer
IT	ItDept
WC	WomenClinic
TGC	Grad College
PRES	PresOff

#### Installing McAfee Endpoint Encryption

#### 1.0 Purpose

This document sets out to provide the steps needed to install and setup McAfee Endpoint Encryption on a computer

#### 2.0 Scope

This document applies to any computer (desktop and laptop) owned by or operated by OU-Tulsa, associated departments, clinics, offsite clinics and affiliates that connect to the OU-Tulsa network

#### 3.1 Policy

#### 3.2 Agent Deployment

1. Log into ePO Server

	d ne pi manch monentrame.		
c	Policy Orchestrator 4.6	W McAfee	
		An arse Company	
	the Browner row are uping to not surrowed	a supported	
		and the second sec	
the second se	er same		
Per	assesseds		
tan	ngsagai (trgish	•	
	arriant 2000 2012 Mades See, M. Rud	the Reserved View (Inc.	
		And	

(Fig. 1)

2. Click on "System Tree"

	Second Property and and	Australia Detti Taska   Braigi Detara				
wis - HSC	Presets This Group Only	Custorer None	Ouick finds	Acole Clear III		
ina - Sooner	System Name	A Hanaged State	Taga	1P.462-883	User Name	Last Communitation
d .						
	_					

3. Select "Workstations – Tulsa"

Issue Date:	2003-12-01
Last Updated:	2016-06-17
Updated By:	Lisa Mildon
Revision:	2.1

4. Change "Preset:" to "This Group and ALL Subgroups"

tree .	System Straphic Access (All)	gred Clerk Table Dutos Detete				
industry in 1970"	Preset: This Group and All Subgroup	225 • Custors lisne •	Quick Finds out	Anth Dear II Incom		
Inflatations - Essnar	Contem Name	A Restanced State	Tan	18 Address	Liter Tartes	Last Communication
orkalations + Tu'sa	1 8 05.105.01	Hanand	Washedulian	10 133 132 251	N/A	3/7/24 3-35-25 44
atiFound		Hannind	Marketation	10.100.100.000	N/A	STRATE TARGET
	T D OWNER	Hanavad	Washington	10.130 155.551	cond Pall, mad have	3/5/14 1.43.35 PM
	I II OUT MANY	Baragant	Rev Industry	10.133.132.204	N/A	NUMBER REPORT AND
	T II outstates	Hanasar	Navionation	10.130.132.231	N.A.	2/20/14 12/32/21 49
	E 007-303-12	Wanaged	Waristation	10 130 152 237	N/A	3/6/14 3:58:55 PM
	E E OUT-3121-14	Nanagad	Warlatation	10.100.132.220	N/A	3/6/64 6+83+23 098
	E E OUT-3630-13	Nanagad	Workstation	10.130.132.239	167.4	3/0/64 8-33-00 PM
	E (D) 007-2623-16	Managed	Rorkatation	10.130.132.240	197.4	3/6/14 11/32 39 PM
	E OUT-3635-12	Managed	Noriatation	10.130.132.242	0n/2966	3/6/24 6:33:07 PM
	1 E OUT-MON-LE	Banoped	Waristation	10.130.132.234	n/z	3/7/24 8:07:14 AM
		Hanaged	Workstation	10.130.182.229	classing	3/3/24 12(0):82 PH
	1 El our-ses-z	Harlaged	TERRADOUT	10.120.132.233	Casa opin	3/7/14 2104/06 AM
	E 007-2835-20	Nanaged	Workatation	10.130.132.225	N/A	3/7/14 9138-50 AM
	E E OUT-1035-25	Wanagad	Workshatton	10.130.132.219	cicele	3/7/14 9:00:16 AM
	E E our-3636-23	Hanaged	Workshatton	10.130.182.222	N/3.	3/7/54 8/59/42 404
	E E our sess co	Haraged	Werkalation	10-130-132.224	theathran	3/7/54 \$100.23 AM
	E E OUT-2633-24	Hanaget	moniatation	10.130.152.234	Casettore	3/3/14 11/01/39 (W
	1 E OUT-3835-25	Managed	Warkstation	10.130 132.218	shui7623	3/5/14 1114/30 PM
	E E Cur-1835-36	Managed	mortistation	10.130 133.214	wineh7206	1/6/14 6/10/15 PM
	1 0 our-sess-sr	Hanaged	Warkstation	10.130.192.217	adi72724	2/5/14 6:00:28 PM
	E E curranasian	Hanaged	Norkataben	10.130.132.213	874H0092	3/6/14 6123(22.9%
	1 0UT-3129-29	Hanagad	Workstation	10.130.132,214	nels4432	3/6/14 6:00:37 PM
	E E 007-3835-3	Managed	Workstation	10.130.137.241	1/2	3/5/14 11/61/52 PH
	1 D 0/7-3438-34	Harapad	Warlabation	10.130 183 218	mjr:1073	3/4/14 4/08/48 294
	E OUT-2432-31	Hanagari	Providation	10.130.132.203	Casaroon	3/4/24 2103/20 8%
	1 U OUT-3939-32	Nanaged	Workstation	10.130.132.230	N/A.	3/7/54 #104/54 AM

(Fig. 3)

- 5. Enter system name in "Quick Find"
  - a. Click Apply
- 6. Check box next to system name

Heren OVA IT Life   Toron 27712	(1 8+11):25 AM C21"   (saar selden 1)					090 1944
Ageneral Trace • The Degeneration	Darkspoor Systems	The Context Reports Policy Capity Resigned Clark Table Ginus Estats Options • Option Rose •	Queck finds (sub-di-suniag)	Story Clear III Show take	ed scen	_
workations nucl Workations - Soner Workations - Tube Lottlinound	E System Name	▲ Pronyet Date Hangpe	Tage BLALDL, Weskutation	19 Addena 356.135.161.237	Ven Reine	san Gerenariaalue 305/4 futtole AM
		Import Agents           Indef, Datasa on a Engle Tyream.           Modif, Datasa on a Engle Tyream.           Modif, Tata on a Engle Tyream.           In Oliver Tash Agen           In Oliver Tash Agen           In Oliver Tash Agen           In Oliver Tash Agen           In Oliver Tash Agen				
	Chases Columns Column	Brier Agent Lag     Dev Clash Events     Dev Clash Events     Dev Clash Events     Dev Clash Events     Dev Transfer Systems     Dev Clash Events     Dev Clash Events     Dev Clash Events				
Dystem Tive Actions •	Roberts V Management	F Wake to Agents    Fing			1	_

(Fig. 4)

- 7. Click "Actions"
  - a. Select "Agent", "Modify Tasks on Single System"
- 8. Click "Actions"
  - a. Select "Actions", "New Client Task Assignment"

Issue Date:	2003-12-01
Last Updated:	2016-06-17
Updated By:	Lisa Mildon
Revision:	2.1

anan Ort II II'd   Tana 3/7/14 bill	(0 AM COT.) Versi Verken 1 Las.Off	du :			000 8
	and the second second second	NEW YORK			
Sfort Tasks for My Organization > Works	Lations - Take > IT > OUT IT TANLAP				
Present: No Filler	1 Ove	a find and	V Cast		
lask Barre	A Task Type	Status	Inhered Form	Table is Up-Te-Date	Actions
Inhal-DAT Londates	Product Opdate	Enabled	Hy Digastration	Taye	Edit Assignment Finalula
Miles Agent Depiny	Product Deployment	Erablish	Morheletone - Tulke	True	Rdit. familaryment   Deleter
tentityteor, Deploy	Freduct Deployment	trabled.	Workstations - Tulaa	True	Bill Assisting 1 Convin
II Depley Tutes Workstations	Froduct Deployment	Erabled	Workstations - Tulae	Tue	Add Add add and I Coloro
IZ Patch Tulsa Workstations	Product Update	Erabled	Morketations - Tulka	Tur	Edd. Assistement 1 division
Chouse Columns					
Expert All Assignments					
Expert Table					
Seport Assignments					
Rev Cient Tack Assignment	1				
utions + 2 issue					

(Fig. 5)

- 9. Under "Task Type"
- 10. Select "Product Deployment"

	AND REPORTED TO AND A DESCRIPTION OF A D			U U U WINCON
there				
	And Alarman Street Stre			
Chest Task Ausgausen Bu	Mart 1 Sedect Task	a saturda	Linear	
My Organization>Workstate	one - Tuber (Tr-OUT-IT-IANLARy Which client task would you like to	advadula?		
Task to fished be	Product	Task Type	Task Barne	
	McAfee Agent	Holive Agent Statistics	EEGO_V.7.0.0.356	
		Healfee agent Wakeup (Windows only)	REPC_ININGTALL	
		Morar Repuestaries (Windows only)	EEPC_V.7.6.2_DKSTALL	
		Product Deployment	HoAfee_Agent_Deploy	
		Product Lipdate	Steldvisor_Deploy	
			W1 A 1 V Industrial	
			View Selected Taxa	
Constant etc.	The book		Constant See Deep 2 (201	
	() Send this task to only composes which have the for Max any of these tasks. None with And has some of these tags: None with	Gaelig Offerie		

(Fig. 6)

- 11. Under "Task Name"
  - a. Select "Drive\_Encryption\_GO\_Windows\_Install" (the default)
  - b. Click Next
- 12. Change "Schedule Type" to "Run Immediately"
  - a. Click Next

level OVT IT EPO   Tirei 3/7/14	3-33-09 AM CET   User Limitation   Mars. 195			000 9444
These Section Section Section	🖉 🤪 🐾 🔞	<b>il</b>		
	Contract Contract Description	Constraints		
Mr Organization Micricatations - Tal	taar IT+OUT-IT-LANLAP: When do you want this task to run		den 3 Constanteren	
Schodule statum	() Destind			
Schodule type:	Run immediately.			
Dytems	Ohep the tesk if it runs for (1,   hour(s)   1,			
				Deci 100 100 100

(Fig. 7)

- 13. Click Save to deploy the agent
- 14. On the PC to be encrypted, Right-click the McAfee shield icon and select "McAfee Agent Status Monitor"
  - a. Click "Collect and Save Props", then "Check New Policies"
    - i. You should see a message for both the download and the install of the agent
- 3.3 Client Deployment (Refer to section 3.2, Fig. 1)
  - 1. Return to or Log into ePO Server
  - 2. Delete the "EEGO" task
  - 3. Complete steps 1 through 7 from Agent Deployment
  - 4. Select "Actions", "New Client Task Assignment"
  - 5. Under "Task Type"
    - a. Select "Product Deployment"
  - 6. Under "Task Name"
    - a. Select "Drive\_Encryption\_install"
    - b. Click Next
  - 7. Change "Schedule Type" to "Run Immediately"
    - a. Click Next
  - 8. Check all the settings on this screen is correct
    - a. Click Save
  - 9. On the PC to be encrypted
    - a. Right-click the McAfee shield icon and select "McAfee Agent Status Monitor"
    - b. Click "Collect and Save Props", then "Check New Policies"
    - c. When the client has been installed you will see a message that the system needs to log off and a timer will start until it automatically logs off
  - 10. The pre-boot encryption logon process is now in place
    - a. Login as normal for an encrypted computer
  - 11. Once back at the desktop
    - a. Right-click the McAfee shield icon and select "McAfee Agent Status Monitor"
    - b. Click "Collect and Save Props", then "Check New Policies"
    - c. Check on the encryption status
      - i. Right-click the McAfee shield icon
      - ii. Select "Quick Settings"
      - iii. "Show Endpoint Encryption Status"

Issue Date:	2003-12-01
Last Updated:	2016-06-17
Updated By:	Lisa Mildon
Revision:	2.1

3.4 Adding a User to an Encrypted Computer

- 1. Log into ePO Server
- 2. Click on "System Tree"
- 3. Select "Workstations Tulsa"



- 4. Click "Menu"
  - a. Select "Data Protection" b. Select "Encryption Users"





Issue Date:	2003-12-01
Last Updated:	2016-06-17
Updated By:	Lisa Mildon
Revision:	2.1

5. Change "Preset:" to "This Group and All Subgroups"

Anto Trans	Py Department > Workstations - Tales			
	Egolana Dreve Units			
Werkatalises - HDC	Dysteens / Dysteen Uners			And a local state
Wenutationa - Dooner.				
Municulations - Talka	Denies The proce are all subproces	Contraction of Contraction of Contraction	Acov Line	
LouthPound	G System Barne	a lage	1P Address	Last Communication
	E 0.07-1069-33	Moriation .	10 100 150 252	3/7/14 9-39:13 AM
	EI DUT-SERIES	wonatation .	10 130 132 249	3/3/14 11-01/32 PM
	007-3629-30	Workstation	10 130 152 251	3/3/14 3 12:39 PH
	EI 007-3428-11	tephatatop	10.130.152.204	3/7/14 9:45:58 AM
	017-3835-12	Wokalaton	13 130 152 223	2/20/14 12:02:23 AW
	E overses a	wonauton	10 130 138 217	3/9/14 3/38/33 294
	0 001-003-04	teoristion	13 130 152 234	2/6/14 6:22:22 PH
	G 0/7-2629-28	workgration	10 100 177.229	3/6/14 8 22/03 898
	OUT-SEED IN	wokatition	15 130 122 2+0	3/4/14 11 32/28 PH
	0 0/7-3839-57	Wurkatation -	10.130.172.242	2/6/14 9 11:07 214
	10 OVF-2839-18	wokaration	10.130.172.118	5/7/14 9-52/15 AM
	1 OUT-303-19	Workplatten	45 430 172 229	3/3/1+11/01/02 PM
	OUT 3535-3	Wafaiatan	15 120 155 253	3/7/14 3.45.07 Am
	E our stati so	Wyfiaiathry	40 400 182 228	2/7/14 2-30:00 AH
	G 0.7 200 11	trustators	15 135 155 119	3/7/14 3:47:17 AM
	B 0/7-303-32	tor privat articles	40.400.102.222	3/7/(+13-04-43 AM
	U 047-3635-33	Modulation	10 100 182 104	3/7/14 9.50-92 AM
	E out see se	Weilatation	10.100.182.004	3/8/14 11-01-83 7%
	1 OVT-3639-28	Incharation	15 130 183 216	3/3/14 7:14/30 5%
	U OVT 2028-26	Waiteration	10 130 183 214	3/0/14 0-10-20 PM
	GUT-3635-27	Westatation	15 135 133 317	3/6/14 6-09-39 PM
	U 0/7-3439-34	Workelation	10 100 182 213	3/6/14 4-25-32 PM
	UI 007-3625-28	tradiatation	13 130 153 214	2/6/14 4-29-27 018
	EII OUT-3839-3	Workeration	10 100 183 541	3/9/14 11-01-83 PH
	C 0.07-3635-30	Traduction	13,130,172,318	2/4/14 4/27-41 PM

(Fig. 10)

- 6. Enter system name in "Quick Find"
  - a. Click Apply
- 7. Check box next to system name

	Pergeneters Welderber Mar Internet Constants										
kiene - HDC Kiene - Dosner	Dartenet : Dartene	Users top and \$1 Subproces * Out	arts Acces	Dark Keti Sch-Amias	ROV Dest	Show which it rows		Main Fit			
kijne - Talee urić	System Barn	4		Taga REALDS, Wonsteine	1P Address		Last Communication	_			
	TR. Crosse Colo	WN Case(a)									
	C Sequert Dec	yatiyo +									

(Fig. 11)

- 8. Click "Actions"
  - a. Select "Endpoint Encryption"
  - b. Select "Add Users"
- 9. Click the "+" box next to the Users field

Issue Date:	2003-12-01
Last Updated:	2016-06-17
Updated By:	Lisa Mildon
Revision:	2.1



(Fig. 12)

- 10. Change "Preset to "Container and Children"
  - a. Enter the user name in the "Quick Find" field
  - b. Click "Apply"

		ici -				
		tink as 10540 becades of				
nan zeen		Contrast (Construction of Construction)	Contract of the local division of the local	94/J	and the second se	
	III Xanerica.	A Design of the second s	Biers Destud in 2,000 renues	-1	The rest	
		2 mil	Container and children *	Quek finds	Acoly B transferred	
			Trans.	and an	Participation of Party	
			10 and black	Ann Mary	Charles New All all an industry and Date T. O Industry	
			II ten shite	Same up ba	Cliniters white Cliniters and a clinite state of the second	
			LI A PATA THEY	A OUT, THET	CRIME FRITE TREET OUNTERE Associate OUNT, OUNTerport	
			11 Aleminat	an order	Clinitester OurTest Insuris OurT. Outlements D	
			13 14845	AURA	Chronikia Ocer/Filiptes, Ourfconyrte, DCrises, DCreek, D	
			U MONDIE	apprender	CII+LED-BOVE OU+EarniseAccounts. DU+I*. OU+Accounts	
			ED AARCONVL	ALECOPYS	ClassifiCOP1.0045cap.0.046anados.ets.00417.01	
			B AARCOPYS	ALBCORVO	ClinitECCP/2.00+Ecspc.Out=Envirolment-role.000+EC.01	
			E AMCORYS	AARCORVE	ClinkaRCOIV3. DUrfropp. D.Unilawijakovusta. DU+IT. DI	
			E AARTODYA	AABCCOPY4	CN+448CCDVA.00+Resp. DJ#GarvesLemonts.00+IT.01	
			E AAGEE	AADEE	ClinALOFF OUrDisabled Accounts.00+IT.0UnAstroute.C	
			E AADSARWI	AADDARWIT	Cli+&ADDARW1.DU+AHSases.0U+Arcounts.0C+hec.0C+	
			EI AALAHE	AALAEE	CENAUARE.CUNARRains.CONArrowts.DChina.COnauLi	
			EI AAPPEL	AAFPEL.	CII+AAPPEL.CU=Disabled Accounts.CU=IT.OU+Accounts.	
			D ARCWER	A6OW28	CIE-ABOWER.DU+Deabled Accesses.DU+ET.DU+Access	
			B ARROY	ABRECHT	CN+XEPECHT.OU+Disabled Accounts.OU+IT.OU+Account	
			ARROWN11	ABROWNED	CII+ABROWILLOU+AMINEEE.00+AMINEME.CC+MeLOC+	
					the second se	

(Fig. 13)

- 11. Check box next to user name you want to add to system
  - a. Click OK
  - b. Click OK again
- 12. Add Tulsa-DesktopAdmins and if clinical PC, add Tulsa-MedInfoAdmins
  - a. See step 8, but click on the "+" next to the field labeled "From the groups" (See Fig. 11)
- 13. On the encrypted PC
  - a. Right-click the McAfee shield icon and select "McAfee Agent Status Monitor"
  - b. Click "Collect and Save Props", then "Check New Policies"
- 14. Enter the new user name at the Encryption logon to test that they are recognized by the Encryption Agent
  - a. The end user will need to reset their security questions when they first logon

#### 4.0 Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action within the appropriate existing University employment guidelines.

 Issue Date:
 2003-12-01

 Last Updated:
 2016-06-17

 Updated By:
 Lisa Mildon

 Revision:
 2.1

5.0 Definitions Term Definition

6.0 Revision History

#### Inventory Updating Procedure

#### 1.0 Purpose

To provide the required steps and guidelines required to update the inventory records within Service Now

#### 2.0 Scope

To achieve and maintain consistency in recording when any hardware or software is deployed, re-deployed or sent to surplus. Also, to record additional features such as warranty status and software licensing

#### 3.1 Policy

3.2 Applies to

• All OU-Tulsa Information Technology employees

#### 3.3 When to record/update

- When new hardware or software is deployed
- When hardware or software is re-deployed to different users and/or locations
- When hardware is sent for surplus
- When licensed software is installed or removed from a computer
- When a warranty (or service contract) is renewed/extended
- After working on a particular endpoint.

#### 3.4 What to record/update

- The information will vary depending on what item(s) are being recorded into Service Now
- To enter or update information within Service Now, first locate the Base Items section of the Configuration menu left side of your screen when looking at the Service Now window



- For this example, to show the required fields, I have opened the Computer option and selected New from the toolbar
  - o Fill out as much information as you can for the item being added or updated
  - o Click the Submit button when you have filled out or updated the relevant sections

.

Issue Date:	2013-01-14		
Last Updated:	2013-03-07 Lisa Mildon		
Updated By:			
Revision:	1.1		

Name:       RAM (MB):         OS Domain:       Disk space (GB):         Manufacturer:       CPU manufacturer:         Model ID:       CPU type:         Os Service Pack:       CPU count:         OS Version:       CPU count:         Imentory Tag:       Encrypted         Status:       - None         Out Of Warranty:       Service Tag:         Status:       Service Tag:         Status:       Service Tag:         Created:       Immetory Tag:	Computer					Su	ıbmit 🔋 🔲 🛱
OS Domain: Disk space (GB):   Manufacturer: CPU manufacturer:   Model ID CPU type:   Operating System:None   OS Senice Pack: CPU speed (MHz):   OS Version: CPU count:   Inventory Tag:None   Status:None   Out Of Warranty:None   Created: Senice Tag:   Status: Senice Tag:   Status: Senice Tag:   Status: Senice Tag:   Created: Immediated Senice Tag:	Name:				RAM (MB):		
Manufacturer:     CPU manufacturer:     CPU type:       Model ID     CPU type:     CPU type:       Operating System:     -None •     CPU count:     1       OS Service Pack:     CPU count:     1       OS Version:     Encrypted     Immentory Tag:     Immentory Tag:       Status:     -None •     Assigned to:     Immentory Tag:       Out Of Warranty:     Immentory Tag:     Service Tag:       Created:     Immentory Tag:     Service Tag:	OS Domain:				Disk space (GB):		
Model ID:     Image: CPU type:     Image: CPU type:       Operating System:     - None     CPU speed (MHz):       OS Service Pack:     CPU count:     1       OS Version:     Encrypted     Image: CPU type:       Image: CPU count:     Encrypted     Image: CPU type: CPU count:       Status:     - None     Encrypted     Image: CPU count:       Status:     - None     Assigned to:     Image: CPU count:       Out Of Warranty:     Image: CPU count:     Service Tag:       Serial Number:     Serial Number:     Image: CPU count:       Created:     Image: CPU count:     Image: CPU count:	Aanufacturer:		Q		CPU manufacturer.		Q
Operating System: None •   OS Service Pack: CPU speed (MHz):   OS Version: CPU count:   OS Version: Encrypted   mentory Tag: Encryption Date:   Status: None •   Out Of Warranty: •   Serice Tag: Serial Number:   Serial Number: Serial Number:   MAC Address: •	Model ID			Q	CPU type:		
OS Service Pack:     CPU count:     1       OS Version:     Encrypted     Immenory Tag:       Inventory Tag:     Immenory Tag:     Encryption Date:       Status:     None •     Assigned to:       Out Of Warranty:     Service Tag:       Serial Number:     Serial Number:       MAC Address:     Immenory	Operating System:	- None	•		CPU speed (MHz)		
DS Version: Inventory Tag: Status: Out Of Warranty: Created: Created: Interprete	OS Service Pack:				CPU count:		1
Immentory Tag:     Encryption Date:       Status:     - None       Out Of Warranty:     Assigned to:       Senice Tag:       Senial Number:       MAC Address:	OS Version:				Encrypted	12	
Status: None  Assigned to: Out Of Warranty: Service Tag: Serial Number: MAC Address: Created:	inventory Tag				Encryption Date:		
Out Of Warranty: Senice Tag: Senial Number: MAC Address: Created:	Status:	None			Assigned to:		Q
Created:	Out Of Warranty:				Senice Tag:		
Created:					Serial Number:		
Created:					MAC Address		
	Created:		-				
	Relations						

#### 4.0 Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action within the appropriate existing University employment guidelines

5.0 Definitions Term Definition

6.1 Revision History

## **Inventory Surplus Procedure**

**<u>Purpose</u>**: This procedure provides the rules and guidelines for proper surplus of equipment.

**<u>Scope:</u>** To achieve and maintain consistent standards for inventory surplus.

#### **Definitions:**

<u>Data Device</u> – Designation for any item that has data storage (PC hard drive, networked printer, etc.)

#### Procedure:

- 1. **Collection** IT staff will remove surplus items from support departments, colleges, and/or clinics as requested. A ServiceNow request must be submitted and approved by user prior to removal of surplus items from owner's location.
  - a. Change of inventory will be noted in Service Now when the item is removed from its owner's location.
  - b. Remove computer object from Active Directory, when applicable.
  - C. All items must be logged on the Inventory Surplus Form when they are brought to desktop staff in the Tech East area. The form can be found: <u>here</u>
  - d. For items with a university asset tag, the IT Business Office must be notified in order to complete a change of inventory form.
- 2. Data Collection If hardware has a hard drive, system information <u>must</u> be recorded and placed in secure storage by CS staff. All data devices can be delivered to CS staff for inventory and storage.
  - a. CS staff will remove hard drive from surplus items and bring to inventory station located at the north end of tech area next to data center.
  - b. Open Hard drive inventory spreadsheet found here
  - C. Scan hard drive serial number with barcode scanner.
  - d. Place host name, reason for disposal, service tag, date and time of disposal and technician's name in spreadsheet fields. If item has an Asset tag that should be noted also.
  - **e.** Hard drive will be placed in secured HiTech Assets container. The combination for the container is on file in the Business Office.
- 3. Sorting CS tech will store all non-data equipment in room 4WB120. When designated surplus shelves have been filled, equipment will be moved to pallets located in south end of garage (with a number color sticker on it) to be shrink wrapped and stored until removal.
  - a. Off-site techs will store non-data storing equipment in their offices until a surplus day is designated.
  - Storage media must be brought to East Tech area at Schusterman. (See step 2)

- 4. Removal CS tech will notify Client Services Manager when 6 or more pallets have been created or data device container is full. Client Services Manager will coordinate removal of assets with IT Business Office. Prior to removal of any equipment, IT Business Office must have a copy of surplus inventory information. This information will be stored on the Tulsa IT SharePoint Site located <u>here</u>.
  - a. For data device IT Business Office will contact HiTech Assets (<u>rmooring@htassets.com</u>) for pick-up of container (HiTech Assets Gaylord box) to have data devices shredded. A new container will be left to replace the full container.
  - b. For non-data surplus IT Business Office will contact HiTech Assets to pick up the pallets of surplus.

#### Compliance:

The Client Services Manager will randomly review inventory database status, the current status of the surplus processes, reports, and activities to ensure that they meet the support standards set in this protocol. Since any hardware that is unaccounted for is a potential breach, accountability of each step in this procedure will be consistently monitored before surplus is removed from central IT area. Anyone responsible for skipping any of these steps will be held accountable with potential disciplinary actions taken.

#### ANY changes to this protocol should result in a copy being sent to the OU- Tulsa Risk Management office.

## **Tripwire Procedure**

- I. On Fridays, CS Security Tech receives weekly vulnerability report.
- II. ServiceNow automatically generates incident for vulnerability remediation
  - A. Request: Request
  - B. Category: Security
  - C. Subcategory: Risk Assessment
  - D. Service: Vulnerability Scan\Remediation
  - E. ITIL Watch list: IT-Security Team
- III. CS Security Tech attaches weekly report.
- IV. CS Security Tech looks at Risk Matrix for a Host Score of 1000 or higher.
  - A. Are there vulnerabilities?
    - 1. If no, then step g.
    - 2. If yes, follow steps below:
      - a. Click on top right corner of Risk Matrix.
      - b. Click on the highest score, on the Affected Hosts number.
      - c. Export vulnerabilities for the current category and attach to SN ticket.
      - d. Determine which items are endpoints.
        - i. Within Tripwire, look at NetBIOS Name or Operating System.
        - ii. Or with NSLOOKUP, NBTSTAT or NMAP via IP address.
        - iii. Compile, export and attach list of endpoints to SN ticket.
      - e. Click on each DNS Name for endpoint vulnerability list.
        - i. Look at Score of each vulnerability, focusing on scores of 1000 or more.
        - ii. Click on each individual Remediation to get definition, instructions and possible download for fix.
          - 1. Research via NIST, US-CERT, TechNET or other pertinent vendor knowledge bases.
          - 2. Paste any research links into SN incident.
        - iii. CS Security Tech downloads any necessary patches or updates for CS Techs to utilize in remediation.
          - If found on non-IT supported systems, contact will be made via SN email to their respective POC support person detailing vulnerabilities.
      - f. CS Security Tech sorts report by NetBIOS Name and creates separate reports to CS Techs for their respective coverage areas.
      - g. CS Security Tech creates new incident per vulnerability and support area based on reports from step e.
        - i. Request Type: Incident
        - ii. Category: Endpoints
        - iii. Subcategory: Security
        - iv. Service: Vulnerability Remediation

- v. Short Description: Vulnerability ID: CVE-#### (pertinent ID issued by Mitre.org.)
- vi. Add CS Security Tech and their respective backup to ITIL Watchlist.
- vii. CS Security Tech attaches report and gives instructions on vulnerability remediation in SN incident.
- viii. In original ticket, CS Security Tech makes note of new Incident numbers.
- h. CS Security Tech notes any new exceptions in original SN incident.
- B. CS Tech performs vulnerability remediation per SN incident.
  - 1. Updates incident and notifies CS Security Tech.
  - 2. CS Security Tech will confirm in the next new scan.
    - a. New scans occur every Thursday; results available on every Friday.
    - b. If all clear, step C.
    - c. If vulnerability still exists, repeat step B.
      - i. If after 2<sup>nd</sup> scan endpoint vulnerability still remains, system will be reimaged.
- C. CS Tech closes their assigned SN incident.
- D. CS Security Tech closes their SN incident.

For full diagram and details, procedure can be found here.