DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

Memo Issued: July 25, 2008
Control #: MITS- 0708-09
Affected IRM: 10.8.20
Expiration Date: 07/31/2009

MEMORANDUM FOR DISTRIBUTION

FROM: /s/ Karen Freeman
                   Director, Information Technology Security

SUBJECT: Interim Guidance – Policy Updates for *Internal Revenue Manual (IRM) 10.8 Section 20, Windows Security Policy*.

This interim guidance memorandum is being issued in order to quickly communicate revised security controls for Windows, as a result of the Federal Desktop Core Configuration (FDCC) security requirements dated June 20, 2008. This policy update also includes additional services necessary for Altiris and SQL Server software.   In order to ensure the currency and relevance of IRS Windows Security Policy, the changes contained herein are being made to IRM 10.8.20, Exhibits 10.8.20-2, 10.8.20-4, 10.8.20-7, 10.8.20-14, 10.8.20-23, 10.8.20-25, and 10.8.20-34.

These requirements shall be distributed to all personnel responsible for ensuring that adequate security is provided for IRS information and information systems. The policy applies to all employees, contractors and vendors of the Service.

1.   **Source(s) of Authority:** IRM10.8.1 is issued in support of TD P 85-01 under the authority of Treasury Directive (TD) 85-01.

2.   **Effect on Other Documents:** Internal Revenue Manual (IRM) 10.8 Section 20, Windows Security Policy.

3.   **Contact:** Please send questions or inquiries related to this guidance to Janice Harrison, Program & Procedures Mgt, MITS Cybersecurity at (202) 283-6762 or Denise Crisco at (631) 447-4515.

4.   **Expiration Date**: This guidance will be incorporated into the IRM 10.8.20 on or before July 29, 2009

Attachment (1)
Interim Guidance - IRM 10.8.20, *Windows Security Policy,* Exhibits 10.8.20-2, 10.8.20-4, 10.8.20-7, 10.8.20-14, 10.8.20-23, 10.8.20-25, and 10.8.20-34.

<u>Distribution</u>
Deputy Commissioner for Operation Support
Deputy Commissioner for Services and Enforcement
Chief, Appeals
Chief, Counsel
Chief, Criminal Investigation
Chief Information Officer

cc: Office of Service-wide Policy, Directives & Electronic Research
<u>www.irs.gov</u>

Attachment (1)

Interim Guidance - IRM 10.8.20, Windows Security Policy, Exhibits 10.8.20-2, 10.8.20-4, 10.8.20-7, 10.8.20-14, 10.8.20-23, 10.8.20-25, and 10.8.20-34

The following change(s) are hereby effective immediately for IRM 10.8.20, Exhibits 10.8.20-2, 10.8.20-4, 10.8.20-7, 10.8.20-14, 10.8.20-23, 10.8.20-25, and 10.8.20-34 *dated March 28, 2008.*

CHANGE(s):
Exhibit 10.8.20-2
(03-28-2008)
Account Policies
Page 54

PASSWORD POLICY			
Account Policy	**XP Workstation**	**2000 Server**	**2003 Server**
Maximum Password Age	**See IRM 10.8.1**	**See IRM 10.8.1**	**See IRM 10.8.1**
Minimum Password Age	**See IRM 10.8.1**	**See IRM 10.8.1**	**See IRM 10.8.1**
Minimum Password Length	**See IRM 10.8.1**	**See IRM 10.8.1**	**See IRM 10.8.1**

ACCOUNT LOCKOUT POLICY			
Account Policy	**XP Workstation**	**2000 Server**	**2003 Server**
Account Lockout Duration	**See IRM 10.8.1**	**See IRM 10.8.1**	**See IRM 10.8.1**
Account Lockout Threshold	**See IRM 10.8.1**	**See IRM 10.8.1**	**See IRM 10.8.1**
Reset account lockout counter after	**See IRM 10.8.1**	**See IRM 10.8.1**	**See IRM 10.8.1**

Exhibit 10.8.20-4
(03-28-2008)
Security Options
Page 57

Security Option	XP Workstation	2000 Server	2003 Server	Reference
Devices: Allow undock without having to log on	**Not Defined**	N/A	Disabled	See IRM 10.8.20.5.2.5.
Devices: Allowed to format and eject removable media *2000 - Allowed to eject removable NTFS media*	**Administrators and Interactive Users** **Note: Registry value = 2 or less is acceptable**	Administrators	Administrators	See IRM 10.8.20.5.2.5. **Administrators and Interactive Users (value = 2)** **Administrators and Power Users (value = 1)** **Administrators (value = 0)**

Exhibit 10.8.20-7
(03-28-2008)
System Directory (C:\Windows (Winnt)\System32) File and Folder Permissions
Page 74

Windows XP and 2003 Server

System Directory File/Folder	User	XP Workstation	2003 Server
%SystemDirectory%\ mshta.exe	Administrators	Full Control	Full Control
	SYSTEM	Full Control	Full Control
	Users	**Read / Execute**	**N/A**

Exhibit 10.8.20-14
(03-28-2008)
Registry Configurations
Page 114, 116

Subject	Information	XP Workstation	2000 Server	2003 Server	Comments
The time in seconds before the screen saver grace period expires	HKLM\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\ Winlogon\ScreenSaverGracePeriod **Type: REG_DWORD**	**Value = 5 or less**	**Value = 5 or less**	**Value = 5 or less**	
Allow Automatic Detection of MTU Size	**Key:** Hkey_Local_Machine\ SYSTEM\CurrentControlSet\ Services\Tcpip\Parameters\ EnablePMTUDiscovery **Type:** REG_DWORD **Value:** = 1 (Recommended) (Enabled) **Value:** = 0 (Default) (Disabled)	**Value = Not Defined**	**Value = Not Defined**	**Value = Not Defined**	

Exhibit 10.8.20-23
(03-28-2008)
System Services
Page 155, 159, 161

Display Name (Service Name)	XP Workstation	2000 Server	2003 Server
Altiris Agent Service (AeXNSClient)	**Automatic**	**Automatic**	**Automatic**
Remote Access Connection Manager (RasMan)	**Not Defined**	Disabled	Disabled
Task Scheduler (Schedule)	**Not Defined**	Automatic	Automatic

Exhibit 10.8.20-23
(03-28-2008)
System Services
Page 163

Services That Shall Not Be Present On a Baseline Server or Workstation

Display Name	Service Name
CWCS TFTP Service	**crmtftp**
CWCS RSH/RCP Service	**crmrsh**

Exhibit 10.8.20-25 (03-28-2008)
Temporary IIS/SQL Settings
Page 168-169

SQL Settings: (Relational Database)
Additions to the System Services Table 10.8.20-23

Display Name (Service Name)	2000 Server	2003 Server
SQLSERVERAGENT	**Automatic**	**Automatic**

Exhibit 10.8.20-34
(03-28-2008)
IRM 10.8.20 FDCC Deviations
Page 196

Remove the following entry for "Remote Access Connection Manager" from Exhibit:

Policy Path	XP Workstation Policy Setting Name	Deviated Setting
Computer Configuration\Windows Settings\Security Settings\System Services	**Remote Access Connection Manager**	**Manual**