

APPENDIX Q

Procedures to Upgrade Security on the Windows NT 4.0 Server and Mintronix P5000 POS

The user is responsible to ensure that all current & required DOIM (or local IMO) Windows NT 4.0 hotfixes, virus protection tools with current signature files, IAVA patches, screensaver, DOD Banner, and service packs are applied to each server and workstation. This document details how to 'increase' security on Windows NT 4.0 Servers and Workstations based upon a thorough scan from an independent source on our AFMIS SCP13-02 test bed. This document is not all-inclusive and will be modified as we learn and discover better ways of protecting the systems.

The following list is what we will discuss in greater detail in this document:

- Change password for the Mintronix & administrator accounts on each POS and Server.
- Rename the administrator account on each POS and Server.
- Change password for the Mintronix user in the NtAutoLogOn.exe program on each POS to one of 8 alphanumeric characters.
- Enable auditing on each POS and the server.
- Modify the account policy for each user on each POS and Server.
- Change the MSSQL default SA account password from null to one of 8 alphanumeric characters.
- Modify System Policy to display DOD banner and to not display last logged on user name.

NOTE: The Mintronix P5000 POS register does not have a keyboard by default and has an automatic login for the Mintronix user. In order to make the changes below you will have to borrow the keyboard from the server temporarily. To login as administrator, you will have to press and hold the '**Shift**' and the '**F10**' keys together as you are logging off as the '**Mintronix**' user. These keys that you hold down will 'break' the automatic login and then you can login as administrator.

How to change the Mintronix & Administrator password on each POS and Server.

- 1) Login as administrator on the POS.
- 2) Click '**Start**', '**Programs**', '**Administrative Tools (Common)**', '**User Manager**'.
- 3) After the User Manager window opens up, highlight the '**Mintronix**' user,
- 4) Then click on '**User**' from the menu.
- 5) Then click on '**Properties**' to open up the properties for the Mintronix user.
- 6) Click or tab to the '**Password**' field.
- 7) Highlight and delete the old password.
- 8) Enter the new 8 alphanumeric character password.
- 9) Click or tab to the '**Confirm Password**' field.

- 10) Highlight and delete the old password.
- 11) Enter the new 8 alphanumeric character password.
- 12) Click on **'Ok'** to apply changes.
- 13) Repeat this process for the administrator account.
- 14) Ensure this task is accomplished on every POS & Server.

How to rename the Administrator account on each POS and Server.

- 1) Login as administrator on the POS.
- 2) Click **'Start'**, **'Programs'**, **'Administrative Tools (Common)'**, **'User Manager'**.
- 3) After the User Manager window opens up, highlight the **'Administrator'** user.
- 4) Then click on **'User'** from the menu.
- 5) Then click on **'Rename'** to open up the **'Rename'** dialog box.
- 6) Enter **'afmisadmin'** in the **'change to:'** field.
- 7) Click on **'Ok'** to apply changes.
- 8) Ensure this task is accomplished on every POS & Server.

How to change the Mintronix password in the NtAutoLogOn.exe program.

- 1) Login as administrator on the POS.
- 2) Open the explorer program by clicking on **'Start'**, **'Programs'**, **'Windows NT Explorer'**.
- 3) Expand the **'Program Files'** folder.
- 4) Expand the **'Maximus'** folder.
- 5) Expand the **'SmartCard Foodservice'** folder.
- 6) Double click on the **NtAutoLogOn.exe** program to open it.
- 7) Change **'User Name'** to **'Mintronix'**.
- 8) Then change the Mintronix password to the same 8 alphanumeric character password that you changed in (1) above, in both the **'Password'** and **'Verify Password'** fields.
- 9) Click on **'Save'** to save changes.
- 10) Click on **'Exit'** to exit the NtAutoLogOn.exe program.
- 11) Repeat this procedure on every POS.

How to enable auditing on POS and Server.

- 1) Login as administrator on POS.
- 2) Click **'Start'**, **'Programs'**, **'Administrative Tools (Common)'**, **'User Manager'**.
- 3) After the **'User Manager'** window opens up, click on **'Policies'** from the menu, and then click on **'Audit'** to open up the **'Audit Policy'** dialog box.
- 4) Check the box called **'Audit These Events'**, then check **'Success'** and **'Fail'** for all seven events.
- 5) Click on **'Ok'** to apply changes. Repeat this procedure on every POS and server.

How to modify the account policy for each user on each POS and Server.

- 1) Login as administrator on POS.
- 2) Click **'Start', 'Programs', 'Administrative Tools (Common)', 'User Manager'**.
- 3) After the **'User Manager'** window opens up, click on **'Policies'** from the menu, and then click on **'Account'** to open up the **'Account Policy'** dialog box.
- 4) Change the **Maximum Password Age** to **'90'**, **Minimum Password Age** to **'89'**, **Minimum Password Length** to **'8'**, and **Password Uniqueness** to **'24'**.
- 5) Check to enable **'Account lockout'**.
- 6) Then change **Lockout after** to **'3'** bad logon attempts.
- 7) Check to enable **Lockout Duration** to **'Forever (until admin unlocks)'**.
- 8) Click on **'Ok'** to apply changes. Repeat this procedure on every POS and server.

How to change the MSSQL default SA account password from null to one of 8 alphanumeric characters.

- 1) Login as administrator on server.
- 2) Click **'Start', 'Programs', 'Microsoft SQL Server 7.0', 'Enterprise Manager'**.
- 3) After the **'Enterprise Manager'** window opens up, then expand the **'SQL Server Group'** folder, expand your **'server's name'** folder, expand **'Security'** folder, double-click **'Logins'**.
- 4) On the right hand side highlight the **'sa'** account and right click, and then click on **'Properties'**.
- 5) Enter an 8 alphanumeric password into the password field.
- 6) Click on **'Apply'**.
- 7) Enter the same password again at the next dialog box.
- 8) Click on **'Ok'**.
- 9) Click on **'Ok'**.
- 10) Close the Enterprise Manager window and reboot the server.

How to change the system policy to display DOD banner & to not display last logged on user name.

- 1) Login as administrator on server.
- 2) Click **'Start', 'Programs', 'Administrative Tools (Common)', 'System Policy Editor'**.
- 3) After the **'System Policy Editor'** window opens up, click on **'File'** from the menu, and then click on **'Open Registry'** to open up the **'System Policy Editor – Local Registry'** window.
- 4) Double click on **'Local Computer'** icon (should already be highlighted).
- 5) In the **'Local Computer Properties'** window, expand the **'Windows NT System'** folder.
- 6) Expand the **'Logon'** folder. Check the box called **'Logon Banner'**.
- 7) Enter a caption for the **'Caption'** field (ex. DOD Warning!!!).
- 8) Enter text for the **'Text'** field (ex. This Computer is For Official Use Only!!!).

- 9) Check the box called '**Do not display last logged on user name**'.
- 10) Click on '**Ok**'.
- 11) Click on '**File**' from the menu, then click on '**Save**'.
- 12) Changes will be saved to registry.
- 13) Close the System Policy Editor window and logoff.
- 14) Try to logon as administrator to test the DOD banner and verify that last logged on user is no only displayed.