**Creating a New Inbound Rule**

**1.** Right-click Start ➢ Control Panel ➢ Large Icon View ➢ Windows Firewall.

**2.** Click Advanced Settings on the left side.

**3.** Right-click Inbound Rules and select New Rule.

**4.** Choose a rule type. For this exercise, choose Custom so you can see all the options

available to you. Then click Next.

**5.** At the Program Screen, choose All Programs. Then click Next.

**6.** Choose the protocol type, as well as the local and remote port numbers that are

affected by this rule. For this exercise, choose TCP, and ensure that All Ports is

selected for both Local Port and Remote Port. Click Next to continue.

**7.** At the Scope Screen, choose Any IP Address for both local and remote. Then click Next.

**8.** At the Action screen, choose Allow The Connection Only If It Is Secure. Click Next.

**9.** At the Users screen, you can experiment with these options if you want by entering

users to both sections. Once you click one of the check boxes, the Add and Remove

buttons become available. Click Next to continue.

**10.** At the Computers screen, you can choose what computers you will authorize or allow

through this rule (exceptions). Again, you can experiment with these options if you

want. Click Next to continue.

**11.** At the Profiles screen, choose which profiles will be affected by this rule. Select one

or more profiles and click Next.

**12.** Give your profile a name and description, and then click Finish. Your custom rule will

appear in the list of inbound rules, and the rule will be enabled.

**13.** Double-click your newly created rule. Notice that you can change the options that

you previously configured.

**14.** Delete the rule by right-clicking the new rule and choosing Delete. A dialog box will

appear asking you if you are sure. Click Yes.