RN Evaluation Procedure

YOU CAN FIND THE EVALUATION TOOL AND RN PEER INPUT TOOL AT THE JIT WEBSITE. Be sure to SELECT THE PERFORMANCE EVALUATION FOR YOUR LEVEL.

Follow the instructions that are attached to the evaluation tool and peer evaluation tool.

Key Dates to remember – the Peer input should be returned to you within 7 days.

- The peer review forms are returned to you. You are to review the content and summarize the information on the performance review form in the peer feedback section of the self-evaluation.
- Peer feedback that is not summarized and included within your performance review form will not be typed in for you.
- Rationale for rating other than “met,” must be provided in the evaluation summary section.
- Self-performance review is to be submitted electronically and will not be typed into the performance review for you.

Upon receiving notification of the annual evaluation, the employee has Three Weeks to complete the self-evaluation (including peer feedback) process. You will submit your completed Staff Performance Planning and Evaluation form and your Peer Review responses via e-mail to the manager (or designee) by (insert date here). If materials are not submitted within two weeks of the due date, the manager may proceed with completing the evaluation process.

You may want to reference the peer input tool when completing your self-evaluation as well as the two documents below:

- Guidelines for overall performance rating
- Performance Evaluation Rating Descriptions

For assistance with the process, see your Manager, Supervisor or Administrative Assistant.

Be sure to include an Annual Plan (Goals) for the next year:

- Goals should be Specific, Measurable, Achievable, Realistic, and Timed.
  - Example: I will become an ONS member by July 20XX.
    1. This goal is
      a. specific – becoming an ONS member,
      b. measurable – either achieved or not achieved,
      c. achievable – not hard to do
      d. realistic – nurse should be able to do this
      e. time – there is a date listed
Directions on how to save/access your own H drive:

**AT WORK**

1. Log in to Novel
2. Click on H drive
3. Click on My Documents

**OUTSIDE OF UMHS**

Different UMHS resources can be accessed remotely in different ways. You can use the Cisco AnyConnect VPN client to access all UMHS resources remotely. Also, subsets of web-based applications are available through an SSL-based browser using the UMHS Level-1 page.

Access via the [Level-1 page portal](https://vpn.med.umich.edu/level1) at the bottom of the University of Michigan Health System home page. The Portal will not work with Internet Explorer version 10 or Windows 8 Operating System. While it should work with web browsers and devices that are not part of the CoreImage environment, currently the page is only supported for Internet Explorer up to version 9.

To ensure easy access within IE, MCIT recommends the following:

1. In Internet Explorer, click **Tools** and select **Options**
2. Click the **Security** tab
3. Select the green **Trusted Sites** icon
4. Click the **Sites** button
5. In the **Add this website to the zone:** box, enter [https://vpn.med.umich.edu/level1](https://vpn.med.umich.edu/level1)
6. Click **Add**
7. Click **Close** on the Trusted Sites dialog box
8. Click **OK** to close the Internet Options dialog box

You may want to install the [Cisco Any Connect VPN](https://vpn.med.umich.edu/level1)

If you have not yet updated your Non-Core device, you can do so using the following instructions:

1. Go to [https://vpn.med.umich.edu/level1](https://vpn.med.umich.edu/level1) and downloading the Cisco AnyConnect client.
2. Log in with your uniquename and level 1 (Kerberos) password.
3. Click on the Start AnyConnect link.

Details are below
Installation Instructions:

Installation

1. Open a web browser and navigate to the following link: https://vpn.med.umich.edu/

2. At the SSL VPN Service screen, provide the following information and click the Login button:
   - **USERNAME:** your UM uniqname
   - **PASSWORD:** your Kerberos (Level-1) password

3. At the message, click the Continue button.

4. Click the Start AnyConnect link.

5. After the installer detects the platform, install the ActiveX control if prompted. Click the Download button.

6. If a message appears indicating the digital signature could not be verified, click the Allow button.
8. The *Windows Installer* window should appear. Installation usually takes a few minutes.

9. When the window indicates a "Connection Established", the installation is complete.

10. On the bottom of the screen, the U of M icon () will be colored blue and yellow to show that it is activated.

11. Connect to the VPN using your uniqname and level one (kerberos) password.

### Using the Cisco AnyConnect Client

After installing the client, the connection can be turned on and off by using the UM logo status icon in the lower right part of the screen.

- **Starting the VPN connection**
  1. Click the UM logo () in the lower right corner of the screen and select **Connect**.
  2. When the *Cisco AnyConnect VPN* window opens, enter your uniqname and kerberos password.

- **Stopping the VPN connection**
  1. Click the UM logo () in the lower right corner of the screen and select **Disconnect**. Alternatively, double-click the UM logo ()
Client window appears, enter your uniqname and Kerberos (Level-1) password.

3. Once connected, the UM logo status indicator will be colored blue and yellow (). This color combination indicates that computer successfully connected to the VPN.

and, when the Cisco AnyConnect VPN Client window appears, click the Disconnect button.

2. Once disconnected, the UM logo status indicator will be colored gray and blue (). This color combination indicates that computer is NOT connected to the VPN.