

Guidelines and Procedures for access to eNETS II Administrative & Report Portal

A) Purpose:

The purpose of this policy is to provide suggestions, based on current best practices, for creating user accounts on and defining access control to eNETS II Administrative and Report Portal. The intention is to reduce the risk of data access by unauthorized people.

B) Guidelines & Procedures for:

i) Group and Role Creation

- The Group and Role creation will ONLY be assigned to those who need access the portal as part of their job responsibilities. All requests must be supported by the requestor's Head of Department and final approval given by the eNETS business unit. The eNETS business unit reserves the rights to deny access to functions requested by the user if it's deemed as irrelevant to the perceived job scope or conflicts with other function rights assigned to the user.
- All requests must be made through the "eNETS II End-User Request Form".
- The System Administrator (eNETS Customer Support) will create an account for the user based on the given sign-offs in the "eNETS II End-User Request Form". The System Administration shall assign an initial, strong password to the account, and upon the first login, the user shall be prompted to change the password.

ii) Account Creation

- The account creation will ONLY be assigned to those who need access the portal as part of their job responsibilities. All requests must be approved by the requestor's Head of Department and Head of Department must decide if the staff need the access before approving the request.
- All requests must be made through the "eNETS II End-User Request Form".
- The System Administrator (eNETS Customer Support) will create an account for the user based on the given sign-offs in the "eNETS II End-User Request Form". The System Administration shall assign an initial, strong password to the account, and upon the first login, the user shall be prompted to change the password.

iii) Update to functions

- Access to additional functions must be approved by the requestor's Head of Department and Head of Department must decide if the staff need the access before approving the request.
- All requests must be made through the "eNETS II End-User Request Form".
- The System Administrator (eNETS Customer Support) will assign the additional functions based on sign-offs in the "eNETS II End-User Request Form".

iii) Deletion of Users

- The System Administrator (eNETS Customer Support) will remove access (on the last day of service) for staff who have resigned (based on eMail notification sent by the HCM Department).
- Another instance where access will be deleted is when the user is assigned a different job scope that no longer requires access to the portal.
- In this case, the request must be made through the "eNETS II End-User Request Form".

