SaILS NSIR-RT Installation Instructions (Docker)

- You will need to create a "secret settings" file specific to your installation:
  - Change into the `sails-app/src/ils/ils/` directory
  - A template version of a secret settings file is provided (`template_secret_settings.py`)
  - Copy this file to a new `secret_dev_settings.py` or `secret_prod_settings.py` file depending on whether creating a development or production environment
  - Edit the following settings within the file you just created:
    - `EMAIL_USE_TLS`
      - Default setting is `True`, but for some servers with significant firewall-ing, may need to set as `False`
    - `EMAIL_HOST`
      - Edit this setting to reflect the email server you wish to use.
      - A production version should use an internal email server for confidentialy reasons.
        - o Enter the IP address of the email server as a string, e.g: `"127.0.0.1"`
        - o For a development version, you may use gmail for example: `"smtp.gmail.com"`
    - `EMAIL_HOST_USER` and `EMAIL_HOST_PASSWORD`
      - If using a service like gmail, provide the email address and password for the desired account
      - If using an internal service, you may be able to omit these settings (delete or comment-out)
    - `EMAIL_PORT`
      - The port number through which the email server runs
    - `CONTACT_EMAIL, NOTIFICATIONS_EMAIL, and DEFAULT_FROM_EMAIL`
      - Provide the valid email address that will appear in the "From:" tag on emails generated by SaILS (likely that of your internal overseer of the incident learning program)
    - `DATABASES`
      - If not using MySQL, you will need to change the `ENGINE` setting
      - Provide the username and password to be used for reading/writing from the database in the `USER` and `PASSWORD` settings
    - `ALLOWED_HOSTS`
      - For production environments, this is a list of strings representing the host/domain names that SaILS will serve. Likely this will just be the IP address of your server, but may include an aliased name for your server if applicable
    - `SECRET_KEY`
      - Create a string to be kept secret
    - `PHP_DIR`
      - The directory (URL) at which PHP scripts connecting to the EMR may be accessed
      - Update once connection with EMR has been established
    - `TUTORIALS`
      - holds the URLs and URL text for links to user tutorials (how to use reporting interface, investigation interface, etc.)
      - Update once tutorials have been created & served (e.g. on DepDocs)
    - The following setttings should be updated with appropriate usernames once internal roles have been designated (the meaning of each is described in the file):
      - `INVESTIGATOR_ANONYMOUS`
      - `INVESTIGATOR_ADMIN`
      - `INVESTIGATOR_THERAPY`
      - `INVESTIGATOR_DOSIMETRY`
      - `INVESTIGATOR_PHYSICS`
      - `INVESTIGATOR_ONCOLOGY`
      - `ILS_MANAGERS`

- An interface for administrators (superusers) of SaILS is provided:
  - Access via: `http://127.0.0.1:8080/admin`
  - Administrators can create/modify users, options for fields, etc. from here
- To add options for the Functional Work Area field (via the admin interface):

- Access: `http://127.0.0.1:8080/admin/incidents_nsir/functionalworkarea/`
- Click “Add functional work area”
- Provide a Name of the ward/unit (e.gs. Brachytherapy, TrueBeam 1, Treatment Planning, etc.)
- Set Order as 1
- Click Save
- Repeat for all relevant functional work areas from which incidents may be reported

Once installed, two prominent features of SaILS will not yet be active:

1. Connection with your deparment EMR
   - This functionality has only been developed for ARIA (version 11.0)
   - Please refer to the instructions provided in :
     `sails_nsir/ils/incidents_nsir/php_templates/README.txt`
2. Automated email reminders for incomplete investigations & actions
   - Please refer to the instructions provided in:
     `sails_nsir/ils/supervisor/SaILS_Installation_Automated_Emails.pdf`