



NRE USER ROLES AND SECURITY MODEL

Organisation and Contract Group:

- Users of the NRE can only be a member of one organisation and belong to a single Contract Group.
- For the majority of users their organisation and Contract Group will have the same name. When an organisation procures a NRE license on behalf of another, for example local or central government on behalf of a voluntary organisation, these will differ. In this case the users organisation could be British Red Cross, but the Contract Group could be the local County Council or the Cabinet Office.
- The following are examples of organisations:
 - West Yorkshire Police
 - Surrey County Council
 - Environment Agency
 - Cabinet Office
 - British Telecom
 - British Red Cross
- These are legal entities which procure accounts/services within the NRE. The organisation defines the number of accounts, connection method, services and resources available to its users.
- All organisations must agree to the NRE Service Specification and sign the Connection Agreement to be allowed access to the NRE.
- Within the Contract Group users are known as members unless they are a Sponsor in which case they undertake the role of administrators.
- Users from other Contract Groups can be co-opted into the group as guests. A user can be a guest of many groups but, is only a member of their own Contract Group.

Forum Group:

- Multi agency organisations, such as resilience groups who have no contractual relationship with the NRE, can request the formation of a Forum Group. A Forum Group is formed from administrators and guests drawn from the Contract Groups. Examples of Forum Groups are:
 - West Yorkshire LRF
 - South East RRF

Note: A Group can have more than one administrator if required



Sponsor:

- The sponsor functions mainly take place in the NRE Portal.
- The sponsor is the organisations point of contact for the NRE with Ultra Electronics and the Civil Contingencies Secretariat.
- They are able to create and delete accounts, reset passwords and issue digital certificates if required.
- They can also administer organisations Contract Groups
- They should also be the first point of contact for users within an organisation if they have any issues before contacting the NRE service desk.
- Every Contract Group must have at least one sponsor.
- Sponsors **must** be named users.
- It is advisable to have more than one sponsor per organisation for resilience purposes. There is nothing to stop every user in your Contract Group being a sponsor although every user would then have maximum privilege levels within the Portal.

This role requires attending a one day training course.

Group Administrator:

- The Group administrator's functions take place within Collaborate.
- The Group Administrator can create and assign users to workgroups, and give them Functional Access Levels.

See also the sections entitled "Functional Access Levels" and "Workgroup Security Levels" for more details on these.

- Sponsors can be Group Administrators as well, although they do not have to be.
- A Group Administrator can administer more than one Group if they wish, providing that they are added as a Group Administrator to the appropriate Groups via the Portal

This role requires attending a one day training course (incorporated with Sponsor training)



User:

- A User is anyone who accesses the NRE either with a named or role based account. All Users, no matter what their privilege levels, must agree to the code of practice for the NRE – the End User Security Agreement.
- A User is by default a member of his Contract Group which has provided his account and he can be a guest of other Groups or subscribe to other Groups.

NRE Portal:

- This is the environment for administering Users' accounts.
- After a successful login to the NRE, the Portal is the area that is presented to the user.
- The portal layout is displayed dynamically depending on whether or not they are a Sponsor. This will determine the amount of functionality available to them within the NRE Portal.
- This is where all Users can review documents such as the End User Security Agreement or the Service Specification. It will also include the DPA and FOI policies for the NRE.
- If the User is a Sponsor then they will have the functionality to create new User accounts and reset passwords etc.
- All Users will be able to access the services available to them from within the NRE Portal e.g. "Collaborate" or "AIMS" depending upon their level of subscription.

Functional Access Levels:

- The Functional Access Level (FAL) determines whether users can read and write, open or create delete folders, documents, events and/or briefings etc. within Collaborate.
- Each group will have a number of FALs, set up by default. These are:
 - Administrator
 - Member
 - Guest
 - Subscriber
- Default FALs are associated with a User's type from the Group assignment in the Portal. This default FAL cannot be removed from the User.
- Further FALs can be created and setup by a user with Group Administrator privileges who will use a tree structure to enable and disable the functional features of the application.



- The “Administrator” FAL will be assigned to Group Administrators and will allow full access to functionality within the group
- The “Member” FAL will be assigned to Contract Group Members when created and will be modifiable once the group has been created. They will have slightly reduced functionality compared to the “Administrator” FAL by default and they can (with the exception of the “Administrator” FAL) be edited from this default.
- A “Guest” FAL by default is identical for member FAL and applies where a User is a “Guest” of other Groups.
- The “Subscriber” FAL will be used for NRE users who are not part of the group but subscribing to information e.g. “What’s New” being produced by the Group. This FAL will have the least amount of functionality by default but can be edited by the Group Administrator.

Workgroup Security Levels:

- A Group Administrator will create Workgroups which may be definitions of roles in the Group (i.e. Flooding, CBRN Planning and Telecoms). The Administrator will then apply one or more Workgroups to each User when they are added to the Group. Default Workgroups are applied according to User type from the Portal and cannot be removed.
- When a users adds data to the system (i.e. adding a new document) a section within the meta-data form will allow you to determine the access each workgroup has to the specified data, this is the Workgroup Security Level (WSL) for this particular item of data, which means each and every item of data on the system has its own unique WSL.
- The permissions section will be applied to each workgroup and allow the following functions for that workgroup to be applied to the data:
 - **Security control:** Allows access to change security on the data.
 - **Modify:** Ability to Read/Write & change details of the data.
 - **Write:** Read & update the data.
 - **Read:** Only read the data.
 - **None selected:** No access to the data.
- The permissions are in order of “highest level of access”. This means that someone with **modify** access will also have **write** and **read** access and someone with **write** access **but not modify** access will have only **write** and **read** access.