IMI roles and responsibilities

1. INTRODUCTION 2

2. AUTHORITY ROLES 2

2.1. NATIONAL IMI COORDINATORS 2
2.2. ACCESS MANAGERS 2
2.3. COORDINATORS 3
2.4. AUTHORITIES 3

3. USER ROLES (ADMINISTRATIVE & CONTENT-RELATED) 4

3.1. THE ADMINISTRATOR ROLE 4
3.2. USER ROLES FOR DIFFERENT MODULES (CONTENT-RELATED ROLE) 4
3.2.1. ROLES FOR INFORMATION REQUESTS 5
3.2.2. ROLES FOR NOTIFICATIONS & ALERTS 5
3.2.3. ROLES FOR REPOSITORIES (DATABASES & REGISTERS) 6

1. INTRODUCTION

This guide tells you about the various types of authorities registered in IMI and their roles. It also explains the roles that can be assigned to individual users.

2. AUTHORITY ROLES

Four roles played by authorities are outlined below. However, it is important to understand that a single authority may be assigned all or some of the roles - or just one.

2.1. NATIONAL IMI COORDINATORS

Each Member State has one National IMI Coordinator or **NIMIC**, whose responsibilities are set out in the IMI Regulation[1]. The NIMIC's role is to make sure IMI operates smoothly by:

- registering the appropriate authorities
- managing access to different modules
- supporting users and ensuring the efficient functioning of IMI.

Depending on the national structure, a NIMIC may choose to delegate some of these responsibilities to other authorities, e.g. registering authorities, by assigning them the role of **Access Manager**. It may also delegate content-related assistance by assigning the role of **Coordinator** for specific modules (so that they can help ensure timely and effective handling of requests, notifications or alerts).

2.2. ACCESS MANAGERS

All NIMICs are automatically Access Managers and can designate other authorities to take on this role (see above).

An Access Manager carries out administrative tasks and can:

- register authorities (and users) in IMI
- manage data and users for existing authorities
- grant and remove access to the different IMI modules
- manage the introduction of new modules (by registering new authorities for the module and/or enabling existing authorities access to the new module).

[1] Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC (‘the IMI Regulation’)

2.3. COORDINATORS

The role of linked-coordinator may be assigned to one or more authorities for a particular module. This role involves monitoring information exchanges and may mean approving outgoing requests, replies, notifications or alerts for the authorities to which the Coordinator is linked. In the case of the information request it can also mean handling requests referred by the sending or receiving authority for assistance.

An authority may be registered as Coordinator for one module (e.g. Services notifications) but may simply act as an authority for another module (e.g. Posting of workers information request). An authority registered as a Coordinator for a particular module can also perform any of the tasks of a regular authority for that module (e.g. drafting and sending an information request).

WORKFLOW	COORDINATOR (linked-coordinator)	AUTHORITY
Information requests	Monitors requests Approves requests (optional)* Handles referrals*	Handles requests (sends, receives & replies to requests, etc.)
Notifications & alerts	Monitors notifications & alerts Approves & broadcasts notifications & alerts* Disseminates notifications & alerts*	Handles notifications & alerts (sends notifications & alerts, comments & attaches documents, etc.)
Repositories (Databases & registers)	∅	Records entries in repositories

These tasks may be performed by users with* ***Approver* *rights only and for exchanges to which the coordinator is linked (see section 3 on User roles).*

2.4. AUTHORITIES

The main actors in IMI are the competent authorities in the EU and Iceland, Liechtenstein and Norway (the European Economic Area) that use the system to exchange information with their counterparts. Depending on their competences and their access rights in IMI, they send and receive requests for information, notifications or alerts, and manage entries in repositories (such as Cash in Transit Licences or the Registers Directory).

If an authority is registered in IMI with access to a given module, but does not have the role of Coordinator, it is considered to play an 'authority' role for that module.

3. USER ROLES (ADMINISTRATIVE & CONTENT-RELATED)

Since the authorities registered in IMI vary considerably in size and organisation the system is flexible. A small authority handling relatively few requests may register just one or two users to perform all tasks in IMI (preferably **at least 2, for back-up**). Conversely, an authority such as a Medical Chamber handling a high volume of requests, might register several IMI users with different user rights. A registered IMI user belongs to only one authority.

3.1. THE ADMINISTRATOR ROLE

Every authority in IMI has at least 1 user with the Administrator role. The first user registered for an authority is automatically assigned this role, which may also be assigned to other users.

Users with Administrator rights can:

- update data about their authority
- register additional users
- manage all the authority's users (including removing users, editing user data, changing user rights and resetting passwords).

An Administrator in an authority with the Access Manager role can also register new authorities in IMI and manage access rights, authority data, and users for other authorities.

ADMINISTRATORS IN AN ACCESS MANAGER	ADMINISTRATORS IN AN AUTHORITY
Register new authorities Invite authorities to self-register & validate their registration	Self-register
Grant authorities access to new modules	∅
For own authority & **for other authorities**: - Manage authority data - Manage users (register, update and remove users, and reset passwords)	For own authority: - Manage authority data - Manage users (register, update and remove users, and reset passwords)

⚠ Authorities are recommended to have **at least 2 users with Administrator rights** - it is important to have a backup for managing user access such as resetting passwords and registering new users.

3.2. USER ROLES FOR DIFFERENT MODULES (CONTENT-RELATED ROLE)

The following table shows the user roles for different types of information exchange.

	INFORMATION REQUESTS	NOTIFICATIONS / ALERTS	REPOSITORIES
Viewer	✓	✓	✓
Handler	✓	✓	✓
Approver*	✓	✓	
Allocator	✓		

**Only authorities designated as Coordinators for a particular module can have users with the Approver role.*

3.2.1. ROLES FOR INFORMATION REQUESTS

Users with **Viewer** rights can view or print the full details of requests sent or received by their authority (including personal data), but cannot take action on the requests.

Users with **Handler** rights can send and reply to information requests on behalf of their authority. Each authority with access to a request module must have at least one request handler.

An **Allocator** can assign requests to particular request handlers on the basis of subject matter or other criteria. Such allocation is typical of larger competent authorities handling many requests. When activating the allocation process, an authority needs to have at least 1 allocator. The authority's Administrators are automatically assigned allocator rights, which they may decide to assign to other users.

The above user profiles may be held in any authority with access to a request module, including authorities acting as Coordinators for information request (request coordinators).

An **Approver** profile can **only** be held by **Coordinators**. These users are responsible for approving outgoing requests and/or replies for those authorities subject to approval. Approvers also handle any requests referred for assistance. Referrals are a way of escalating a disagreement between authorities over an information exchange. Each Coordinator must have at least one user designated as Approver.

3.2.2. ROLES FOR NOTIFICATIONS & ALERTS

Viewers can see the full details of all notifications and alerts sent or received by their authority. They can print them, but cannot, for instance, send or respond to them.

Handlers deal with notifications and alerts on behalf of their authority. They can initiate notifications/alerts and submit them to a coordinator for approval. They also receive notifications/alerts and can react to them (add comments, upload documents).

However, they cannot broadcast or disseminate them, even if their authority is a Coordinator for the module concerned.

The **Approver** role can be held **only** by users in an authority acting as **Coordinator** for the module concerned. These users are responsible for approving and broadcasting notifications or alerts and for disseminating them within their own country. To be able to draft and submit notifications or alerts, an Approver must also have the handler role.

3.2.3. ROLES FOR REPOSITORIES (DATABASES & REGISTERS)

Viewers can see the full details of the repository entries to which their authority has access. They can consult and print the details of entries, but cannot, for instance, create or edit one.

Handlers manage repositories and directories on behalf of their authority. They can create new repository entries and activate (publish) them in IMI. They can also edit or deactivate entries, depending on the specifics of the repository in question.