ve

**Lawful Agency User Manual v 1.0**

* **Central Equipment Identity Register Portal**

Document Change History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change Type | Description | Date |
| Draft |  | Submitted for internal review | June 2020 |

Contents

[1 Overview 1](#_Toc43398092)

[1.1 Scope 1](#_Toc43398093)

[1.2 Acronyms & Abbreviations 1](#_Toc43398094)

[1.3 Conventions 1](#_Toc43398095)

[2 Operations 3](#_Toc43398096)

[2.1 Application Overview 3](#_Toc43398097)

[2.2 Logging into the Application 3](#_Toc43398098)

[2.3 Application User Interface 10](#_Toc43398099)

[2.3.1 Dashboard 12](#_Toc43398100)

[2.4 Reporting Stolen/Recovered Devices 16](#_Toc43398101)

[2.4.1 Reporting Individual Stolen Devices 16](#_Toc43398102)

[2.4.2 Reporting Company/Organization/Government Stolen/Lost Devices 23](#_Toc43398103)

[2.5 Reporting Recovered Devices 30](#_Toc43398104)

[2.5.1 Reporting Individual Recovered Devices 30](#_Toc43398105)

[2.5.2 Reporting Company/Organization/Government Recovered Devices 35](#_Toc43398106)

[2.6 Editing Stolen or Recovered Device Requests 40](#_Toc43398107)

[2.7 Filtering Stolen or Recovered Device Requests 41](#_Toc43398108)

[2.8 Exporting Stolen or Recovered Device Requests 42](#_Toc43398109)

[2.9 Grievance Management 43](#_Toc43398110)

[2.10 Filtering Grievances 47](#_Toc43398111)

[2.11 Exporting Grievances 48](#_Toc43398112)

Figures

[Figure 1: DMC Home Page 3](#_Toc43398113)

[Figure 2: Lawful Agency Registration 4](#_Toc43398114)

[Figure 3: Verify OTP 6](#_Toc43398115)

[Figure 4: Enter OTP 6](#_Toc43398116)

[Figure 5: Login 7](#_Toc43398117)

[Figure 6: Home Page 8](#_Toc43398118)

[Figure 7: Forgot Password 8](#_Toc43398119)

[Figure 8: Set New Password 9](#_Toc43398120)

[Figure 9: Home Page 10](#_Toc43398121)

[Figure 10: Edit Information 11](#_Toc43398122)

[Figure 11: Change Password 11](#_Toc43398123)

[Figure 12: Manage Account 12](#_Toc43398124)

[Figure 13: Home Page 13](#_Toc43398125)

[Figure 14: Home Page 15](#_Toc43398126)

[Figure 15: Home Page 16](#_Toc43398127)

[Figure 16: Stolen/Recovery 17](#_Toc43398128)

[Figure 17: Report Stolen (Individual) 18](#_Toc43398129)

[Figure 18: Error File 23](#_Toc43398130)

[Figure 19: Home Page 23](#_Toc43398131)

[Figure 20: Stolen/Recovery 24](#_Toc43398132)

[Figure 21: Report Stolen (Company/Organization/Government) 25](#_Toc43398133)

[Figure 22: Home Page 30](#_Toc43398134)

[Figure 23: Stolen/Recovery 30](#_Toc43398135)

[Figure 24: Report Recovery (Individual) 31](#_Toc43398136)

[Figure 25: Home Page 35](#_Toc43398137)

[Figure 26: Stolen/Recovery 36](#_Toc43398138)

[Figure 27: Report Recovery (Company/Organization/Government) 36](#_Toc43398139)

[Figure 28: Stolen/Recovery 40](#_Toc43398140)

[Figure 29: Stolen/Recovery 41](#_Toc43398141)

[Figure 30: Filtered Requests 42](#_Toc43398142)

[Figure 31: Stolen/Recovery 42](#_Toc43398143)

[Figure 32: Open or Save Stolen/Recovery File 43](#_Toc43398144)

[Figure 33: Exported Stolen/Recovery File 43](#_Toc43398145)

[Figure 34: Home Page 44](#_Toc43398146)

[Figure 35: Grievance Management 44](#_Toc43398147)

[Figure 36: Report Grievance 45](#_Toc43398148)

[Figure 37: Grievance Management 46](#_Toc43398149)

[Figure 38: Filter Grievances 47](#_Toc43398150)

[Figure 39: Filtered Grievances 48](#_Toc43398151)

[Figure 40: Grievance Management 49](#_Toc43398152)

[Figure 41: Open or Save Exported Grievance File 49](#_Toc43398153)

[Figure 42: Exported Grievances 49](#_Toc43398154)

# Overview

## Scope

The objective of this manual is to help lawful agency personnel report stolen and recovered devices (IMEIs/MEIDs/ESNs) and report grievances.

## Acronyms & Abbreviations

| **Acronym** | **Full Form** |
| --- | --- |
| CEIR | Central Equipment Identity Register |
| EIR | Equipment Identity Register |
| ESN | Electronic Serial Number |
| IMEI | International Mobile Equipment Identity |
| MEID | Mobile Equipment Identifier |
| PDA | Personal Digital Assistant |
| TAC | Type Allocation Code |
| TRC | Telecom Regulator of Cambodia |

## Conventions

| **Information** | **Convention** |
| --- | --- |
| UI elements  (such as names of windows, buttons, and fields) | Bold |
| References  (such as names of files, sections, paths, and  parameters) | *Italics* |
| **\*** | Indicates a mandatory field or column |

# Operations

## Application Overview

The CEIR Lawful Agency Portal application enables agency personnel to report devices (IMEIs/MEIDs/ESNs) that are stolen and report devices (IMEIs/MEIDs/ESNs) that are recovered. This includes devices owned by individuals, companies, organizations, and government.

Lawful agency personnel can use the application to perform the following tasks:

* Report stolen devices (IMEIs/MEIDs/ESNs)
* Report recovered devices (IMEIs/MEIDs/ESNs)
* Report grievances

## Logging into the Application

Before login, personnel need to register in the application.

To register:

1. Enter the DMC home portal page URL in the browser address bar. This opens the following page.

A screenshot of a cell phone

Description automatically generated

Figure 1: DMC Home Page

1. Select **Lawful Agency** from the **Registration** list.

The **Lawful Agency Registration** page appears. The personnel need to enter the following information.

A screenshot of a social media post

Description automatically generated

Figure 2: Lawful Agency Registration

1. **\*First Name**: Enter the first name.
2. **Middle Name**: Enter the middle name (if any).
3. **\*Last Name**: Enter the last name.
4. **Address**: Enter the address:
   * Street Number
   * Village
   * Locality
   * District
   * Commune
   * Postal Code
   * Country
   * Province
5. **\*National ID:** Enter the national ID of the agency personnel.
6. **\*Upload National ID**: Upload the image of the original national ID of the personnel. This can be a pdf or image (.jpeg) of size not more than 2 MB.
7. **Upload Photo**: Upload the photograph of the personnel. The photograph can be a pdf or image (.jpeg) of size not more than 2 MB.
8. **Employee ID**: Enter the employee ID.
9. **Upload ID Card**: Upload the image of the ID card. The photograph can be a pdf or image (.jpeg) of size not more than 2 MB.
10. **Nature of Employment**: Select the type of employment of the personnel:
    * Permanent
    * Temporary
    * Contract
11. **Designation and Title**: Enter the designation of the agency personnel.
12. **Reporting Authority Name**: Enter the name of the officer to whom the personnel reports to.
13. **Reporting Authority Email ID**: Enter the mail ID of the officer to whom the personnel reports to.
14. **Reporting Authority Contact Number**: Enter the contact number of the officer to whom the personnel reports to.
15. **Email**: Enter the mail ID of the personnel. This mail ID would be used for communication with the agency
16. **\*Contact Number**: Enter the mobile number of the personnel. The agency would receive notifications at this mobile number.
17. **\*Password**: Enter a login password. This is the password that would be used to log into the Lawful Agency Portal application.
18. **\*Retype Password**: Re-enter the password for confirmation.
19. **\***Select three security questions and enter an answer for each question. This is required by the system when the agency personnel forget the login password. In such a situation, the system requires some type of identification to authenticate the personnel. The security questions are used to identify and authenticate the personnel.
20. **\***Enter the captcha shown on the page. This is required to prove to the system that the personnel are not a robot.
21. **\***Select the declaration check box.
22. Click **SUBMIT**.

An OTP is sent to the personnel’s mail ID and contact number.

A screenshot of a cell phone

Description automatically generated

Figure 3: Verify OTP

The personnel are prompted to enter both the OTPs in the page for verification.

A screenshot of a cell phone

Description automatically generated

Figure 4: Enter OTP

If the two OTPs match, the following message appears. If the OTPs do not match, an error message is displayed. In case the OTP is not received, click **Resend OTP** to request the CEIR system to resend the OTP. The two OTPs are resent, one to the contact number and the other to the mail account.

A screenshot of a social media post

Description automatically generated

After the OTPs are verified successfully, the registration request is sent for approval to the CEIR administrator. The approval turnaround time is 2-3 days. After approval from the CEIR administrator, an e-mail containing a registration ID is sent to the agency’s personnel mail account. The registration ID is a unique automatically generated ID. The ID is the login username for access to the CEIR Lawful Agency Portal application. This concludes the registration process.

To start using the application, log into the application.

To login:

1. Open the browser and enter the DMC home portal URL in the address bar. The login screen appears.

A screenshot of a cell phone

Description automatically generated

Figure 5: Login

On the top right corner of the login screen is the **Language** option. The application supports two languages: **English** and **Khmer**. On selecting a given language, all the field and column labels in the application appear in the selected language. All user inputs are, however, in English.

A screenshot of a cell phone

Description automatically generated

1. Next, enter the assigned login user ID and password.

User ID is the registration ID that is sent on mail to the personnel after successful registration in the system. User ID is a unique ID that is automatically generated by the system. The login password is the password that the personnel enters in the registration page. Refer to during *Figure 2: Lawful Agency Registration*.

1. Enter the captcha.
2. Click **LOGIN**.

If the login and password are incorrect or the captcha is not correct, an error message appears, and the personnel is prompted to re-enter the login details.

On entering correct information, the application Home page appears.

A screenshot of a computer

Description automatically generated

Figure 6: Home Page

If the personnel forget the assigned password, click the **Forgot Password** link on the **Login** page. The **Forgot Password** page appears.

A screenshot of a cell phone

Description automatically generated

Figure 7: Forgot Password

1. Enter the login user ID.
2. Select a security question from the list. Select any one of the security questions that were selected during registration.
3. Enter the answer to the selected security question. This should match the answer given at the time of registration.
4. Click **SUBMIT**.

The **Set New Password** page appears.

A screenshot of a cell phone

Description automatically generated

Figure 8: Set New Password

1. Enter a new password. Click  to see the password characters being entered. Click on it again to hide the password characters. This works like a toggle key.
2. Re-enter the password.
3. Click **Save**.

## Application User Interface

On logging into the application successfully, the CEIR Lawful Agency Home page appears.

A screenshot of a computer

Description automatically generated

Figure 9: Home Page

The Home page has all the feature menus on the left panel.

The center of the page is the Dashboard.

The top right corner of the screen displays the following menu options:

* **Download Manual** : Click to download this user manual.
* **English** : Select **English** or **Khmer**. All the field and column labels appear in the selected language. User inputs are, however, in English.

A close up of a logo

Description automatically generated

* **Home**: Click on it to go to the **DMC Home Portal** page.
* A close up of a logo

  Description automatically generated (**User profile**): Click on it to see the following menu:

A screenshot of a cell phone

Description automatically generated

* **** (**Edit Info**): Click on it to modify the registered information. The **Edit Information** page opens.

A screenshot of a computer

Description automatically generated

Figure 10: Edit Information

1. Make the required changes.
2. Click **Submit** to save the changes.

* **** (**Change Password**): Click on it change the login password.

A screenshot of a cell phone

Description automatically generated

Figure 11: Change Password

1. **Old Password**: Enter the existing password. Click  to see the password characters being entered. Click on it again to hide the password characters. This works like a toggle key.
2. **New Password**: Enter a new password.
3. **Confirm Password**: Re-enter the new password to confirm the password.
4. Click **SUBMIT**.

* **** (**Enable/Disable Account**): Personnel can deactivate their account or disable/enable their account.
  + Deactivating an account means deleting the login account. After the account is deleted, he/she can raise a grievance to reactivate it when required. The grievance is sent to the CEIR administrator who reactivates the account. After reactivation, the personnel can use the same login username and password to log into the application.
  + When the account is disabled, the personnel can only view information and not add or modify information in the application. After the account is disabled, they can enable it using the same menu.

A screenshot of a cell phone

Description automatically generated

Figure 12: Manage Account

1. Select **Deactivate** or **Disable**.
2. Click **SUBMIT**.

### Dashboard

The Dashboard provides a quick display and access to the following information:

* Stolen/Recovery
* Grievance Management

**A screenshot of a computer

Description automatically generated**

Figure 13: Home Page

**Grievance**

The box displays the total number of grievances registered by the personnel.

A screenshot of a cell phone

Description automatically generated

Click  (**View**) to go to the **Grievance Management** dashboard. Refer to *Grievance Management* for more information.

**Stolen Requests**

This box displays the total number of requests reported for stolen devices (IMEIs/MEIDs/MSNs).

A screenshot of a cell phone

Description automatically generated

Click  (**View**) to go to the **Stolen/Recovery** dashboard. Refer to *Stolen/Recovery Devices* for more information.

**Stolen Device Count**

This box displays the total number of devices (IMEIs/MEIDs/MSNs) that have been reported as stolen.

A screenshot of a cell phone

Description automatically generated

Click  (**View)** to go to the *Stolen/Recovery* dashboard.

**Recovery Requests**

This box displays the total number of device recovery requests that have been reported by the personnel.

A screenshot of a cell phone

Description automatically generated

Click  (**View)** to go to the *Stolen/Recovery* dashboard.

**Recovery Device Count**

This box displays the total number of devices (IMEIs/MEIDs/MSNs) that have been recovered.

A screenshot of a cell phone

Description automatically generated

Click  (**View)** to go to the *Stolen/Recovery* dashboard.

**Notification Information**

This section displays the ten most recent notifications.

**A screenshot of a computer

Description automatically generated**

Figure 14: Home Page

Notifications are of two types.

1. Notifications that provide only information. For example, a notification informing the personnel about the account status is an information only notification because it requires no action. The **View** icon () is disabled in such notifications.
2. Notifications that require some action by the personnel. For example, a notification about a rejection of a stolen device request requires the personnel to take some action. The **View** icon () is enabled in such notifications. Click  (**View)** to access the relevant request details.

The notification panel has the following columns:

* **Date**: Date of sending the notification
* **Transaction ID**: Transaction ID for which the notification is sent. If the notification is related to the personnel account (activation, deactivation), the login username is shown instead of any transaction ID.
* **Feature**: This is the name of the feature for which the notification is sent. For example, if the notification is for a grievance, the feature name **Grievance** is shown.
* **Message**: This is the message of the notification.
* **Action**: This shows the **View** icon. It is activated  if the personnel can click on it else it is disabled .

## Reporting Stolen/Recovered Devices

Lawful agency personnel report devices that have been stolen and recovered. The device could belong to an individual or a company/organization/government.

### Reporting Individual Stolen Devices

To report an individual stolen device:

1. Select **Stolen/Recovery** in the left panel of the Home page.

**A screenshot of a computer

Description automatically generated**

Figure 15: Home Page

The **Stolen/Recovery** dashboard appears.

A screenshot of a social media post

Description automatically generated

Figure 16: Stolen/Recovery

1. Click **Report Stolen/Recovery** (seen on the top right corner of the menu bar).

A screenshot of a cell phone

Description automatically generated

1. Select **Stolen**.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a cell phone

Description automatically generated

Figure 17: Report Stolen (Individual)

The screen has two sections: **Individual** and **Company/Organization/Government**.

By default, the **Individual** section appears. Here, the devices that are stolen from an individual are reported.

1. Enter the following information:

**Personal Information:** Enter the personal details of the person whose stolen device is reported.

* \*First Name
* Middle Name
* \*Last Name
* \*Upload NID/Passport Image: Click **Select** to upload an image or pdf of the document.
* \*NID/Passport Number: Enter the NID or passport number.
* \*Email: Enter the mail ID.
* \*Alternate Contact Number: Enter the mobile number.
* \*Address (Property Location)
* \*Street Number
* \*Village
* \*Locality
* \*District
* \*Commune
* \*Postal Code
* \*Country
* \*Province

**Device Information**: Enter details of the stolen device.

* \*Device Brand Name: Select the brand of the device from the list.
* \*Device ID Type: Select the type of ID to be entered for the device:
  + IMEI
  + MEID
  + ESN
* \***Device Type**: Select the type of device from the list.
* \***Model Number**: Enter the model number of the device.
* \***Contact Number**: Enter the contact number of the operator.
* \***Operator**: Select the operator name from the list.
* **Multiple SIM Status**: Select whether the device supports multiple SIM slots.
  + Yes
  + No
* \***Complaint Type**: Select the type of complaint (Lost, Stolen) from the list.
* **Blocking Type**: Select the blocking mode. This is applicable only to blocking:
  + Immediate: The device is instantly blacklisted.
  + Default: The device is sent to the blacklist after a given duration. The duration is configurable by the CEIR administrator.
  + Later: The device is sent to the blacklist at the specified date. Select the date using the calendar A picture containing clock, door, drawing

    Description automatically generated.
* **IMEI/MEID/ESN**: Enter the value of the IMEIs or MEIDs or ESNs of the device stolen/lost.

**Place of Device Stolen**: Enter the address of the place where the device was stolen or lost.

* \*Address (Property Location)
* \*Street Number
* \*Village
* \*Locality
* \*District
* \*Commune
* \*Postal Code
* \*Country
* \*Province
* \***Device Stolen Date**: Click on the calendar A picture containing clock, door, drawing

  Description automatically generated to select the date.
* **Upload FIR**: Click **Select** to upload the FIR file.
* **Remark**

1. Click **Submit**.

A unique transaction ID is generated, and the request is processed internally. The request can be seen on top of the dashboard.

For each request, the dashboard displays the following information:

| **Column** | **Description** |
| --- | --- |
| Date | Date of registering the request. |
| Transaction ID | Transaction ID assigned to the request. |
| Request Type | Type of request generated is Stolen. |
| Mode | Indicates whether the request is for an individual or company (Individual or Company). In this case, it is Individual. |
| Status | * The request goes through the following status modes:   + New: When a request is raised, the status is New.   + Processing: The request is verified internally.   + Rejected by System: If the request has an error, an error file is generated. The error file can be downloaded. The error could be in the file format, size, policy violation or request specifications.   + Pending Approval from CEIR Admin: If the request is successfully verified by the system, the request is shared with the CEIR administrator for review.   + Rejected by CEIR Admin: The CEIR administrator reviews the details and rejects the request if there is a problem. The operator can view the error file and fix the errors in the request.   + Approved by CEIR Admin: When the CEIR administrator approves the request, the status changes to Approved by CEIR Admin.   + Withdrawn by CEIR Admin: When the CEIR administrator withdraws the request, the status changes to Withdrawn by CEIR Admin. For example, this could be done when the personnel have wrongly marked a device as stolen, which has been recovered.   + Withdrawn by User: The personnel can withdraw the request only when the status is New or Rejected by System. |
| IMEI Quantity | Refers to the number of IMEIs reported stolen or recovered. |
| Quantity | Refers to the number of devices reported stolen or recovered. A device can have multiple IMEIs/MEIDs/ESNs. |
| Action | This displays different actions that can be performed on the request.   * Error : An error file is generated if there is any problem in the request(s) submitted. Click to download the error file. Refer to *Figure 18* for a sample error file. * Download A circuit board    Description automatically generated: This is applicable only when the request is for company/organization/government stolen devices. This opens the input device file that is uploaded to the system. * View : This is used to view the request. Click on it view the request details. * Edit A close up of a logo    Description automatically generated: This is used to modify the request. This is allowed only when the status is New or Rejected by System or Rejected by CEIR Admin. Click on it to modify the request details. * Delete : This is used to delete the request. This is allowed only when the request status is New or Rejected by System. Click on it to delete the request. * View History: This is used to view the history of the transaction. It shows the various status modes through which the transaction has gone through. |

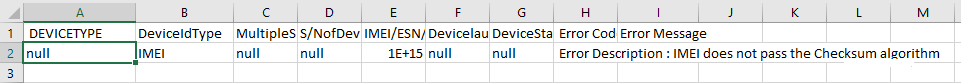


Figure 18: Error File

### Reporting Company/Organization/Government Stolen/Lost Devices

To report a stolen device:

1. Select **Stolen/Recovery** in the left panel of the Home page.

A screenshot of a computer

Description automatically generated

Figure 19: Home Page

The **Stolen/Recovery** dashboard appears.

A screenshot of a social media post

Description automatically generated

Figure 20: Stolen/Recovery

1. Click **Report Stolen/Recovery** (seen on the top right corner of the menu bar).

A screenshot of a cell phone

Description automatically generated

1. Select **Stolen**.
2. Click **Report Stolen/Recovery** (seen on the top right corner of the menu bar).

A screenshot of a cell phone

Description automatically generated

1. Select **Stolen**.

Select the **Company/Organization/Government** tab.

A screenshot of a social media post

Description automatically generated

A screenshot of a cell phone

Description automatically generatedA screenshot of a cell phone

Description automatically generatedA close up of a logo

Description automatically generated

Figure 21: Report Stolen (Company/Organization/Government)

1. Enter the following information:

* **Company Name**
* **Address (Property Location)**
* **Street Number**
* **Village**
* **Locality**
* **District**
* **Commune**
* **Postal Code**
* **Country**
* **Province**

**Authorized Personnel:** Enter the personal details of the authorized person in the company/organization/government.

* First Name
* Middle Name
* Last Name
* Official E-Mail ID
* Contact Number

**Place of Device Stolen:** Enter the address of the place where the device(s) was stolen/lost.

* Address
* Street Number
* Village
* Locality
* District
* Commune
* Postal Code
* Country
* Province
* **Complaint Type**: The complaint type has two values:
  + Stolen
  + Lost
* **IMEI Quantity**: This is the total count of the IMEIs in the stolen/lost devices.
* **Device Quantity**: This is the total number of devices stolen/lost. A device can have multiple IMEIs.
* **Upload Device List**: Enter the stolen/recovered device details in a **.csv** file and upload it.

A screenshot of a cell phone

Description automatically generated

* **Blocking Type**
  + Immediate: The device(s) is instantly blacklisted.
  + Default: The device(s) is sent to the blacklist after a given duration. The duration is configurable by the CEIR administrator.
  + Later: The device(s) is sent to the blacklist at the specified date. Select the date using the calendar A picture containing clock, door, drawing

    Description automatically generated.
* **Upload FIR**: Click **Select** to upload the FIR file.
* **Remark**

1. Click **Submit**.

A unique transaction ID is generated, and the request is processed internally. The request can be seen on top of the dashboard.

1. For each request, the dashboard displays the following information:

| **Column** | **Description** |
| --- | --- |
| Date | Date of registering the request. |
| Transaction ID | Transaction ID assigned to the request. |
| Request Type | Type of request generated is Stolen. |
| Mode | Indicates whether the request is for an individual or company (Individual or Company). In this case, it is Company. |
| Status | * The request goes through the following status modes:   + New: When a request is raised, the status is New.   + Processing: The request is verified internally.   + Rejected by System: If the request has an error, an error file is generated. The error file can be downloaded. The error could be in the file format, size, policy violation or request specifications.   + Pending Approval from CEIR Admin: If the request is successfully verified by the system, the request is shared with the CEIR administrator for review.   + Rejected by CEIR Admin: The CEIR administrator reviews the details and rejects the request if there is a problem. The personnel can view the error file and fix the errors in the request.   + Approved by CEIR Admin: When the CEIR administrator approves the request, the status changes to Approved by CEIR Admin.   + Withdrawn by CEIR Admin: When the CEIR administrator withdraws the request, the status changes to Withdrawn by CEIR Admin. For example, this could be done when the personnel have wrongly marked a device as stolen, which has been recovered.   + Withdrawn by User: The personnel can withdraw the request only when the status is New or Rejected by System. |
| IMEI Quantity | Refers to the number of IMEIs reported stolen. |
| Quantity | Refers to the number of devices reported stolen. A device can have multiple IMEIs/MEIDs/ESNs. |
| Action | This displays different actions that can be performed on the request.   * Error : An error file is generated if there is any problem in the request(s) submitted. Click to download the error file. Refer to *Figure 18* for a sample error file. * Download A circuit board    Description automatically generated: This is used to take a dump of the **.csv** file that is uploaded to the system. This file is uploaded when the request is for stolen company/organization/government devices. This is enabled when the request is rejected by the system or CEIR Admin. Click on it download the file. * View : This is used to view the request. Click on it view the request details. * Edit A close up of a logo    Description automatically generated: This is used to modify the request. This is allowed only when the status is New or Rejected by System or Rejected by CEIR Admin. Click on it to modify the request details. * Delete : This is used to delete the request. This is allowed only when the request status is New or Rejected by System. Click on it to delete the request. * View History: This is used to view the history of the transaction. It shows the various status modes through which the transaction has gone through. |

## Reporting Recovered Devices

Lawful agency personnel can report devices that have been recovered. The device could belong to an individual or a company/organization/government.

### Reporting Individual Recovered Devices

To report an individual recovered device:

1. Select **Stolen/Recovery** in the left panel of the Home page.

A screenshot of a computer

Description automatically generated

Figure 22: Home Page

The **Stolen/Recovery** dashboard appears.

A screenshot of a social media post

Description automatically generated

Figure 23: Stolen/Recovery

1. Click **Report Stolen/Recovery** (seen on the top right corner of the menu bar).

A screenshot of a cell phone

Description automatically generated

1. Select **Recovery**.

A screenshot of a computer

Description automatically generatedA screenshot of a cell phone

Description automatically generated

Figure 24: Report Recovery (Individual)

The screen has two sections: **Individual** and **Company/Organization/Government**.

By default, the **Individual** section appears. Here, the devices that have been recovered for an individual are reported.

1. Enter the following information:

**Personal Information:** Enter the personal details of the person whose stolen device has been recovered.

* \***Device Brand Name**: Select the brand name from the list.
* **Model Number**: Enter the device model number.
* \***Device ID Type**: Select the ID type to be entered for the device:
  + IMEI
  + MEID
  + ESN
* **Device Type**: Select the type of device recovered.
* **Multiple SIM Status**: Select whether the device supports multiple SIM slots:
  + Yes
  + No
* **Device Serial Number**: Enter the device serial number.
* \*IMEI/MEID/ESN: Enter the IMEI or MEID or ESN number(s) of the device recovered.

**Place of Recovery**

* \*Address (Property Location)
* \*Street Number
* \*Village
* \*Locality
* \*District
* \*Commune
* \*Postal Code
* \*Country
* \*Province
* \***Device Recovery Date**: Click the calendar A picture containing clock, door, drawing

  Description automatically generated to select the date when the device was recovered.
* **Remarks**

1. Click **Submit**.

A unique transaction ID is generated, and the request is processed internally. The request can be seen on top of the dashboard.

For each request, the dashboard displays the following information:

| **Column** | **Description** |
| --- | --- |
| Date | Date of registering the request to recover the device. |
| Transaction ID | Transaction ID assigned to the request. |
| Request Type | The request type here is Recovery. |
| Mode | Indicates whether the request is for an individual or company (Individual or Company). In this case, it is Individual. |
| Status | * The request goes through the following status modes:   + New: When a request is raised, the status is New.   + Processing: The request is verified internally.   + Rejected by System: If the request has an error, an error file is generated. The error file can be downloaded. The error could be in the file format, size, policy violation or request specifications. This is applicable only for company/organization/government recovered devices.   + Pending Approval from CEIR Admin: If the request is successfully verified by the system, the request is shared with the CEIR administrator for review.   + Rejected by CEIR Admin: The CEIR administrator reviews the details and rejects the request if there is a problem. The personnel can view the error file and fix the errors in the request.   + Approved by CEIR Admin: When the CEIR administrator approves the request, the status changes to Approved by CEIR Admin.   + Withdrawn by CEIR Admin: When the CEIR administrator withdraws the request, the status changes to Withdrawn by CEIR Admin. For example, this could be done when the personnel have wrongly marked a device as stolen, which has been recovered.   + Withdrawn by User: The personnel can withdraw the request only when the status is New or Rejected by System. |
| IMEI Quantity | Refers to the number of IMEIs recovered. |
| Quantity | Refers to the number of devices recovered. A single device can have multiple IMEIs/MEIDs/ESNs. |
| Action | This displays different actions that can be performed on the request.   * Error : An error file is generated when there is a problem in the request(s) submitted. Click on the icon to download the error file. * Download A circuit board    Description automatically generated: This is applicable when the request is for company/organization/government recovered devices. This downloads the device file that is uploaded to the system. * View : This is used to view the request. Click on it view the request details. * Edit A close up of a logo    Description automatically generated: This is used to modify the request. This is allowed only when the status is New or Rejected by System or Rejected by CEIR Admin. Click on it to modify the request details. * Delete : This is used to delete the request. This is allowed only when the request status is New or Rejected by System. Click on it to delete the request. * View History: This is used to view the history of the transaction. It shows the various status modes through which the transaction has gone through. |

### Reporting Company/Organization/Government Recovered Devices

To report recovered company/organization/government devices:

1. Select **Stolen/Recovery** in the left panel of the Home page.

A screenshot of a computer

Description automatically generated

Figure 25: Home Page

The **Stolen/Recovery** dashboard appears.

A screenshot of a social media post

Description automatically generated

Figure 26: Stolen/Recovery

1. Click **Report Stolen/Recovery** (seen on the top right corner of the menu bar).

A screenshot of a cell phone

Description automatically generated

1. Select **Recovery**.

Select the **Company/Organization/Government** tab.

A screenshot of a social media post

Description automatically generatedA screenshot of a cell phone

Description automatically generated

Figure 27: Report Recovery (Company/Organization/Government)

1. Enter the following information:

* **IMEI Quantity**: Enter the number of IMEIs recovered.
* Device Quantity: Enter the number of devices recovered. A device can have multiple IMEIs/MEIDs/ESNs.
* **Upload File**: Enter the recovered device details. To enter the device details, click **Download Sample Format** and save the format file. Enter the device details in the specified format. Click **Select** to upload the file.
* **Remarks**

**Place of Device Recovery**: Enter the address of the place where the devices were recovered.

* Address (Property Location)
* Street Number
* Village
* Locality
* District
* Commune
* Postal Code
* Country
* Province
* **Device Recovery Date**: Click the calendar A picture containing clock, door, drawing

  Description automatically generated to select the recovery date.

1. Click **Submit**.

A unique transaction ID is generated, and the request is processed internally. The request can be seen on top of the dashboard.

1. For each request, the dashboard displays the following information:

| **Column** | **Description** |
| --- | --- |
| Date | Date of registering the request. |
| Transaction ID | Transaction ID assigned to the request. |
| Request Type | The request type is Recovery. |
| Mode | Indicates whether the request is for an individual or company (Individual or Company). In this case, it is Company. |
| Status | * The request goes through the following status modes:   + New: When a request is raised, the status is New.   + Processing: The request is verified internally.   + Rejected by System: If the request has an error, an error file is generated. The error file can be downloaded. The error could be in the file format, size, policy violation or request specifications.   + Pending Approval from CEIR Admin: If the request is successfully verified by the system, the request is shared with the CEIR administrator for review.   + Rejected by CEIR Admin: The CEIR administrator reviews the details and rejects the request if there is a problem. The operator can view the error file and fix the errors in the request.   + Approved by CEIR Admin: When the CEIR administrator approves the request, the status changes to Approved by CEIR Admin.   + Withdrawn by CEIR Admin: When the CEIR administrator withdraws the request, the status changes to Withdrawn by CEIR Admin. For example, this could be done when the personnel have wrongly marked a device as stolen, which has been recovered.   + Withdrawn by User: The personnel can withdraw the request only when the status is New or Rejected by System. |
| IMEI Quantity | Refers to the number of IMEIs recovered. |
| Quantity | Refers to the number of devices recovered. A device can have multiple IMEIs/MEIDs/ESNs. |
| Action | This displays different actions that can be performed on the request.   * Error : This is enabled when there is an error file generated because of a problem in the request(s) submitted. Click on the icon to download the error file. * Download A circuit board    Description automatically generated: This is used to take a dump of the **.csv** file that is uploaded to the system. This file is uploaded when the request is for company/organization/government recovered devices. This is enabled when the request is rejected by the system or CEIR Admin. Click on it download the file. * View : This is used to view the request. Click on it view the request details. * Edit A close up of a logo    Description automatically generated: This is used to modify the request. This is allowed only when the status is New or Rejected by System or Rejected by CEIR Admin. Click on it to modify the request details. * Delete : This is used to delete the request. This is allowed only when the request status is New or Rejected by System. Click on it to delete the request. * View History: This is used to view the history of the transaction. It shows the various status modes through which the transaction has gone through. |

## Editing Stolen or Recovered Device Requests

Lawful agency personnel can change the request details registered in the system. This can be done only when the request status is New or Rejected by System.

To modify request details:

1. Click **Edit (**A close up of a logo

   Description automatically generated**)**  against the request to be modified.

A screenshot of a computer

Description automatically generated

Figure 28: Stolen/Recovery

The **Edit** page appears. The page has the same fields as seen in the page when reporting individual or company/organization/government stolen or recovered devices.

1. Make the required changes
2. Click **UPDATE**.

The status of the request changes to **New** and is submitted for reprocessing.

## Filtering Stolen or Recovered Device Requests

Lawful agency personnel can view selective device requests after specifying the required filters. For example, they can view requests that are pending approval from the CEIR administrator.

To filter device requests:

A screenshot of a computer

Description automatically generated

Figure 29: Stolen/Recovery

1. Enter data in one or more of the listed fields:

* **Start** **Date** and **End** **Date**: This refers to the period of reporting stolen/lost or recovered devices.
* **Transaction ID**: Each request is assigned a unique transaction ID.
* **Status**: This refers to the status of the request:
  + New
  + Processing
  + Rejected by System
  + Rejected CEIR Admin
  + Approved CEIR Admin
  + Withdrawn CEIR Admin
  + Withdrawn User
* **Mode**: This refers to whether the request for a stolen or recovered device is: Individual or Company.
* **Request Type**: This refers to the type of request: Stolen or Recovered.

1. Click **FILTER**.

The requests that match the filter values are shown in the dashboard.

A screenshot of a computer

Description automatically generated

Figure 30: Filtered Requests

## Exporting Stolen or Recovered Device Requests

Personnel can download all the uploaded requests in a **.csv** file. This is done using an export utility.

To export the uploaded requests:

1. On the **Stolen/Recovery** page, click **Export**.

A screenshot of a computer

Description automatically generated

Figure 31: Stolen/Recovery

The following page appears.

A screenshot of a cell phone

Description automatically generated

Figure 32: Open or Save Stolen/Recovery File

1. Click **Open with** to view the **.csv** as an Excel file.

A screenshot of a computer

Description automatically generated

Figure 33: Exported Stolen/Recovery File

Filtered data can also be exported. To do this, filter specific data by defining filter values. Refer to *Filter Stolen or Recovered Device Requests* for information and then use the export feature to export the filtered data.

## Grievance Management

Lawful agency personnel can register complaints or grievances when there is a problem in the portal. For example, there could be situations when the stolen/recovery feature is not working.

When the personnel raise a grievance, the grievance goes through the following stages:

1. A notification is sent to the CEIR administrator. The notification appears on the CEIR administrator portal. A mail is also sent to the registered mail of the CEIR administrator.
2. The CEIR administrator responds to the grievance. A response notification is sent to the lawful agency portal, and the registered mail ID.
3. Steps 1 to 2 are repeated until the grievance is closed. The administrator closes the grievance.

There are situations when the grievance is automatically closed. A grievance is automatically closed when the status of the grievance changes to **Pending with User**, but there is no response from the personnel for a specified period.

To raise a grievance

1. Select **Grievance Management** in the left panel.

A screenshot of a computer

Description automatically generated

Figure 34: Home Page

1. The **Grievance Management** page appears. Click **Report Grievance**.

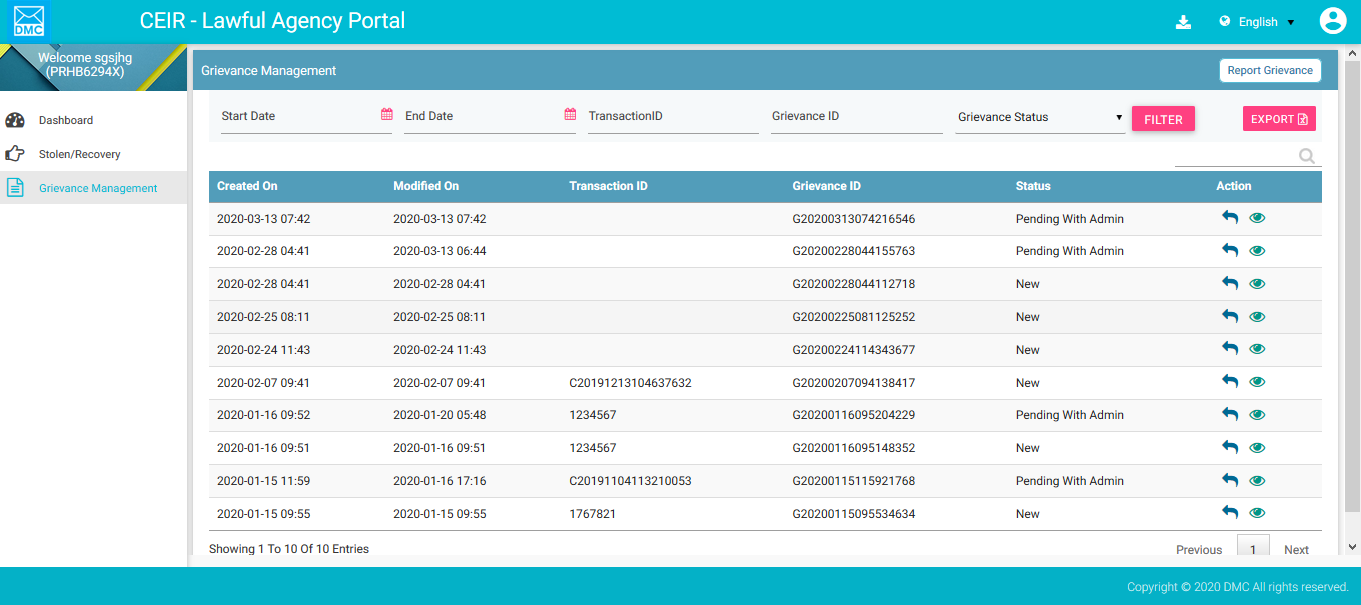


Figure 35: Grievance Management

The **Report Grievance** page appears.

A screenshot of a cell phone

Description automatically generated

Figure 36: Report Grievance

1. Enter the following information:
   1. **Transaction ID**: Enter the transaction ID of the stolen/recovery request if the grievance is related it.
   2. **\*Category**: Select the category of the grievance. The options are:

* Stolen/Recovery Related
* Other
  1. **Document Type:** Select the type of identification or another document that is to be uploaded.
* FIR Document
* National ID Document
* Other
  1. **Upload Supporting Document:** Click **Select File** to upload the document selected in **Document Type**.
  2. To upload more documents,click **+Add More Files.**

This adds two more fields: **Document Type** and **Select File**.

* 1. **\*Remarks:** Enter information about the grievance raised. This helps the administrator to understand the problem in detail.

1. Click **SUBMIT**.

A grievance ID is generated and assigned to the registered grievance. The registered grievance appears on top of the dashboard.

A screenshot of a social media post

Description automatically generated

The new grievance appears on the top of the page.

A screenshot of a social media post

Description automatically generated

Figure 37: Grievance Management

For each grievance added, the following information is displayed on the page.

| **Column** | **Description** |
| --- | --- |
| Created On | Date of raising a grievance. |
| Modified On | The date when the grievance was modified. |
| Transaction ID | The transaction ID of request for which a grievance was raised. |
| Grievance ID | This is the ID that is automatically assigned to the grievance. |
| Grievance Status | The uploaded grievance goes through different status modes.   * New: When a grievance is raised. * Pending with CEIR Administrator: When a response is awaited from the CEIR administrator. * Pending with User: When a response is awaited from the lawful agency personnel. * Closed: When the CEIR administrator closes the grievance. |
| Action | This displays different actions that can be performed on a grievance.   * Reply : This is used to respond to the grievance. The response is given by the CEIR administrator or agency personnel. The exchange of responses is done until the grievance is closed. * View A close up of a logo    Description automatically generated: This is used to view the grievance response history. The agency personnel can see all the responses exchanged for any grievance. |

## Filtering Grievances

The agency personnel can view selective grievances depending on specific filter values. For example, the personnel can view only those grievances that are pending with the CEIR administrator. Similarly, one can view only those grievances that are closed.

To filter grievances:

A screenshot of a computer

Description automatically generated

Figure 38: Filter Grievances

1. Specify the required value in one or more of the fields listed:

* **Start Date** and **End Date**: Period of raising grievances.
* **Transaction ID**: This is the ID of the transaction for which the grievance is raised.
* **Grievance ID**: This is the ID assigned to the grievance.
* **Grievance Status**: The status can be:
  + New
  + Pending with CEIR Administrator
  + Pending with User
  + Closed

1. Click **Filter**.

The filtered grievances are shown on the page.

A screenshot of a computer

Description automatically generated

Figure 39: Filtered Grievances

## Exporting Grievances

All the uploaded grievances can be downloaded in a **.csv** file. This is done using an export utility.

To export the grievances:

1. Click **Export** (seen on the top right corner of the **Grievance Management** page).

A screenshot of a computer

Description automatically generated

Figure 40: Grievance Management

The following page appears.

A screenshot of a cell phone

Description automatically generated

Figure 41: Open or Save Exported Grievance File

1. Click **Open with** to view the file.

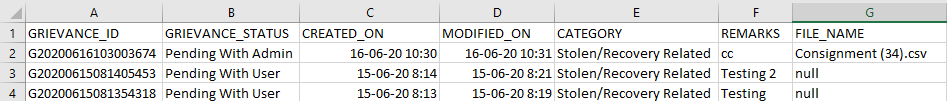


Figure 42: Exported Grievances

Instead of exporting all the grievances, personnel can export filtered grievances. First, filter the grievance data based on specific filters (refer to *Filter Grievances*) and then export the filtered grievances using the export utility.