Case Management System

Investigator/non-Administrator Instructions

Your Lighthouse Services Case Management System (CMS) has been set up and is ready for your use. It is a powerful tool to oversee and manage all your Lighthouse Services hotline reports.

With the CMS you can track every issue from the receipt of an alert through its resolution so you can enhance investigations, oversight and due diligence and create an audit trail.

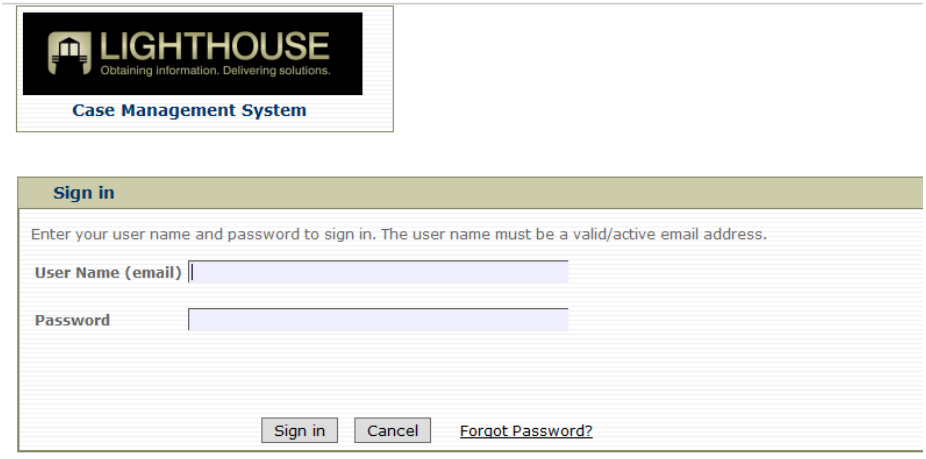
Here are just a few of the CMS features and capabilities:

- View the report online
- Assign Risk Level, Priority and Status
- Record your Follow-up and Outcome
- Dialog with Reporter and Lighthouse
- Manage reports you have been assigned to
- Attach multiple files to a report

Getting Started:

To get the most from your CMS, spend some time exploring its capabilities.

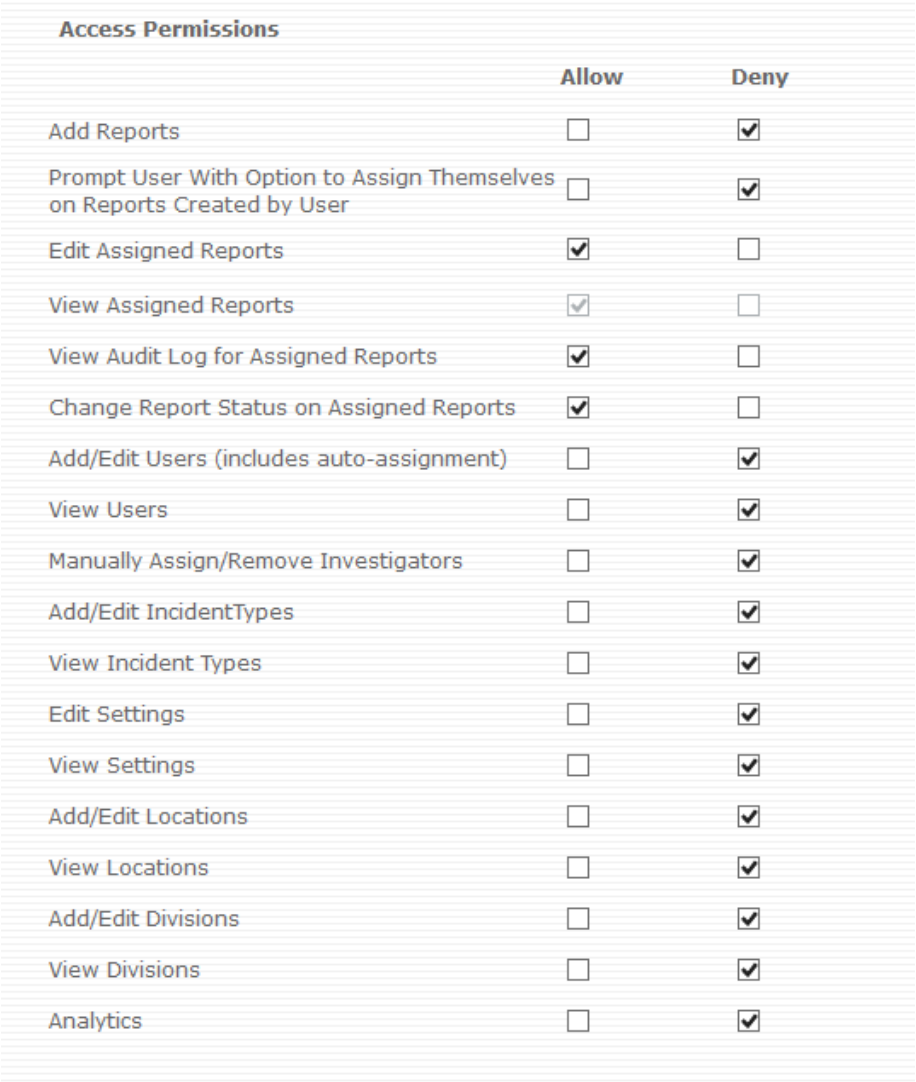
1. Click on this link to access your Case Management System: http://www.lighthouse-services-cms.com. Then enter your User Name (which is your email address) and unique Password. If you forget your password, simply select 'forgot password' below the sign in location.



2. Create a CMS link on your desktop for easy access - open the login page in your browser and drag the address to your desktop. Rename CMS or CMS Login.

3. Start by reviewing the help file and tutorials which have extensive information about how to use this CMS software.
   To view a CMS brochure – click here.
   To view the CMS help file – click here.
   To view a CMS video tutorial – click here.

IMPORTANT – Investigator/non-Administrator User profiles are dynamic and their access permissions can be modified by an Administrator or user with access to the Add/Edit Users setting. Instructions are provided on the basis of the following default access permissions for an Investigator/non-Administrator role:

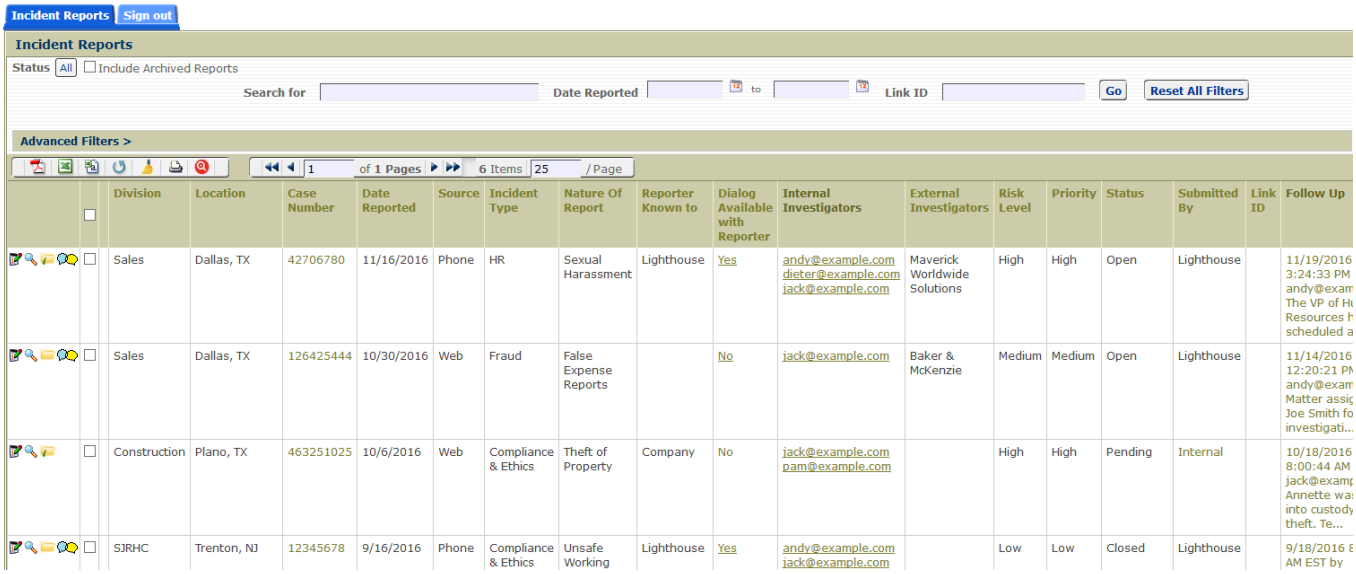


Access Permissions	Allow	Deny
Add Reports	☐	☑
Prompt User With Option to Assign Themselves on Reports Created by User	☐	☑
Edit Assigned Reports	☑	☐
View Assigned Reports	☑	☐
View Audit Log for Assigned Reports	☑	☐
Change Report Status on Assigned Reports	☑	☐
Add/Edit Users (includes auto-assignment)	☐	☑
View Users	☐	☑
Manually Assign/Remove Investigators	☐	☑
Add/Edit IncidentTypes	☐	☑
View Incident Types	☐	☑
Edit Settings	☐	☑
View Settings	☐	☑
Add/Edit Locations	☐	☑
View Locations	☐	☑
Add/Edit Divisions	☐	☑
View Divisions	☐	☑
Analytics	☐	☑

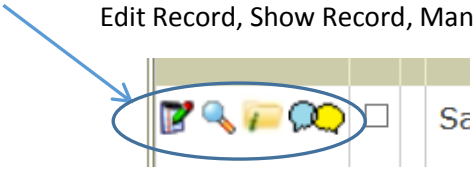
Following the default configuration section you will find a secondary section addressing system features that can be available by modifying an Investigator/non-Administrator's access permissions.

DEFAULT CONFIGURATION

4. **Incident Reports Tab** - The CMS opens in the Incident Reports tab which is the nerve center of the CMS and where you can manage all your Incident Reports. It is here you can review and edit your reports.



There are four icons adjacent to the report that will allow you to manage the report. You are able to Edit Record, Show Record, Manage Files and Manage Dialog in that order.



a. Edit Record - This feature is where you do most of your work and where you are able to edit and document information into the report. Text in grey cannot be edited but can be copied. Text in black can be edited. You can also modify the nature of a report, update the location, link reports, identify an external investigator such as outside auditor, and update the status, risk or priority by using the drop down lists. All updates are time stamped and identify the user who made the change. Also, enter your investigative actions and outcomes here. After entering and saving data in these fields it is time and user stamped and the data cannot be modified.

b. Show Record - By selecting this icon, you will see a comprehensive and non-editable version of the report. You can click Create PDF to download a copy of the entire report.

c. Manage Files – Administrators and Investigators may attach multiple files (Word, PDF, Excel, images, etc.) to the report using the Manage Files icon available in the Incident Report page. If the Manage Files icon includes a green "i" , there is at least one file attached to the report. To add a file to the report, you click on the add icon, browse to locate the file and click save. To view a file, simply click the download button.

d. Manage Dialog - Communication with a reporter or Lighthouse should be entered in the Case Management System dialog feature. There is a column on the Incident Reports page titled Dialog Available with Reporter that indicates if dialog is available directly with the reporter:
   - If YES, please enter your information or questions in the **"Add Dialog for Reporter"** section to communicate directly with the reporter.
   - If NO, enter your information or questions in the **"Add Dialog for Lighthouse"** section. If Lighthouse has the reporter's contact information, we will endeavor to contact the reporter on your behalf; otherwise we will keep your instructions on file in the event the reporter requests a status update.
   - Reports submitted without the PIN option, enter your information or questions for the reporter in the **"Add Dialog for Lighthouse"** section.
   - Occasionally a reporter will request a status update on their report outside of the CMS dialog feature. In that case we will contact your CMS users via the CMS dialog feature to request an update on their behalf.
   - You can use Quick Response Messages to reporters that can be quickly sent or saved for a reporter from the Dialog page. Users can choose which Quick Response Messages to send to the reporter with a few clicks of their mouse (see #8c).
   - Anonymity is determined by the reporter in one of three ways which can be viewed in the 'Reporter Known to' column. The employee may request full anonymity; this means that neither you nor Lighthouse knows the identity of the reporter and the field will be blank. The second option for anonymity is that Lighthouse has been provided the reporter's contact information but it will not be disclosed to you. Finally, a reporter can waive anonymity permitting Lighthouse to disclose the reporter's identity to you.

e. Audit Incident Report - From the Incident Reports page the CMS will allow you to view an audit trail of report activity by using the Audit icon. Select the date range and Case Number. The report information will be displayed by Field Name, New Value, Date Changed and the ID of the user who made the change. You can print or export the audit trail to PDF, Excel or CSV.

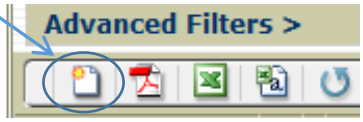
ADDITIONAL FEATURES

The following additional features may be available to an Investigator/non-Administrator if Access Permissions have been allowed.

Incident Reports Tab – Continued

f. Manage Investigators - Assign one or more Administrators or Investigators to an incident report for follow-up and investigation by clicking the Manage Investigators icon and selecting from the dropdown list of system users. An email is automatically sent to an investigator when they are added to or deleted from a report. The CMS is safeguarded with optimistic locking preventing inadvertent overwriting of a record by simultaneous user sessions.

g. Add an internal report – If you receive a report outside of the Lighthouse system and would like to manually add it into the system, click the add icon located on the far left side of the screen. Create a unique report number. Complete the fields. Copy and paste the report text. Then save. By default, only CMS administrators can add internal reports, but investigators can be given permission to add internal reports.



5. **Users Tab** - The system has two levels of users: Administrators, who have complete access throughout the system including all reports, and Investigators/non-Administrators, who are assigned to individual reports by an Administrator.

Company Administrators:

- Have access to the Incident Reports tab as well as Settings, Users, Locations, Divisions, Incident Types, and Analytics tabs
- Can add and delete users and manage user profiles
- Can add and delete divisions, incident types and locations
- Have access to modify their CMS settings and use the analytics feature
- Can access all incident reports, create internal reports, assign investigators, track progress, dialog, add files, etc.

Investigators/non-Administrators:

- Profiles are dynamic and can be modified based on a user's needs
- Default settings:
    - Have access only to the Incident Report tab
    - Can investigate, track progress, dialog, and add files only to reports they have been assigned to
    - Cannot add investigators to reports
    - Cannot create internal reports

The system provides clients with the flexibility to select user roles and adapt their profiles to the needs of their organization.

a. Add New Users - Administrators may set up additional users by selecting the Users Tab. Click the Add icon, enter the user name, email address, and user role, then save. The CMS will send all new users an email notification containing a link to the CMS and the ability to create their password. The email will also contain the "Welcome to Lighthouse Services Case Management System!" information appropriate to their user role.

b. Modify User Access - The CMS gives Administrators the option to modify user access permissions for the Investigator/non-Administrator role. On the User page Investigators/non-Administrators will have a Manage User Access icon next to their user profile. Click to open and manage their permissions. There are 3 default settings: Read Only, Default Investigator and Division Manager. The tool tips provide definitions of each default setting.

You may also select specific permissions from the list and click “allow” or “deny” to enable or disable. Allowing all permissions for an Investigator/non Administrator provides them the same permissions as an Administrator except they will not be allowed to add or delete an Administrator User.

c. Auto-Assign Users to Reports - Selecting the Manage Auto Assignment icon  gives you the ability to have any User in the CMS automatically assigned to a report based on the criteria chosen. When a report is added to the CMS, if all the selected criteria are met, the user will be sent an email notification they have been assigned, automatically be given access to the report and their email address will be added to the Internal Investigator column. From the criteria lists, simply select one or more items and click the Add button. All conditions must be met for the user to be auto-assigned.

d. Resend User Password Info - On the User page selecting the Edit Record icon and then selecting the Send ‘Create User Password Email’ button will allow Administrators to assist users who have forgotten their Sign In credentials by generating an automated email to the user.

e. Reminder Notification to Assigned Users - Create automated email notifications with configurable messages to CMS users assigned as an investigator to a report. When enabled, users assigned to a report receive reminder notification emails when the status of an incident report remains unchanged for a specified period of time. The time intervals and the messages to be sent are defined using the 'Manage Reminder Notifications' page (see #8b)

6. **Incident Types, Divisions and Locations Tabs** - Allow you to standardize your CMS data and enhances your auto-assign criteria. If you require a long list of Divisions or Locations to be added, Lighthouse will provide you with a spreadsheet to complete and then upload them on your behalf.

7. **Analytics Tab** - Provides a dashboard overview of your hotline activity and allows you to generate various reports based on Date Range, Incident Type, Division, Location, Activity Trend, a Benchmark report, and Data Export which allows for exporting a customized set of your hotline data.

8. **Settings Tab** - CMS is configurable allowing you to customize user experience simply by enabling or disabling various features. Use the edit feature to make any changes to your company's settings.

    a. General Settings - CMS is delivered to you with the following default configuration:

Function	Setting	Description
Allow Locations to be Associated with Divisions	OFF	This feature enables an administrator or user with Add/Edit Division permission to associate Locations to one or more Divisions. This will provide filtering of Locations when a Division is chosen on the Add and Edit Incident Report pages.
Suppress Report/Dialog in Emails	OFF	This feature allows Administrators to suppress all dialog and report content within an email from the CMS. By default, report text and dialog are included in the content of CMS emails. If this feature is enabled, emails generated by the CMS between the Company and the Reporter or Lighthouse will only indicate the case number and the sender (Lighthouse or reporter). No other information

		will be included in the email. The Company would then need to sign in to the CMS to view any dialog or report content.
New Incident Report Email Notification	OFF	This feature enables Administrators to be notified via email when a new incident report has been added to the CMS.
Dialog Copy Administrators	ON	This feature allows Administrators to determine if they will receive a copy of dialog updates between the reporter or Lighthouse and the company. When this setting is enabled, Administrators and all assigned investigators will receive an email when the reporter or Lighthouse enters dialog. When this setting is not enabled, only the assigned investigators are sent an email. Note: Regardless of this setting, all administrators are sent an email when no one is assigned to the report.
Email Status Change to Administrator	OFF	When enabled, Administrators are notified of an incident report status change. If no Administrator has been assigned to a report all Administrators are notified.
Allow Deletion of Files Uploaded by Company	ON	This features allows Administrators to permit or prevent users from deleting files uploaded by the company for incident reports. This feature provides users with the capability to delete company-uploaded files for incident reports.
Populate Sender Field on Emails	ON	This feature allows Administrators to receive bounce back messages on failed emails to a user. If this feature is not enabled, Administrators will not receive any notification that a CMS generated email to a user has failed. This feature may need to be disabled if the company's SPAM rules are stringent and will not allow the Sender field to be an email address from their own domain.
Restrict Access to CMS Via IP Address	OFF	This feature allows Administrators to restrict access to CMS via IP Address. If enabled only company specified IP addresses will be able to access CMS.
Enforce Lockout On Unsuccessful Login Attempts	OFF	This feature provides Administrators with the ability to lock a user's account if the user has 5 consecutive failed login attempts. If this feature is enabled, a user's account will be locked after 5 consecutive failed login attempts. The user's account can only be unlocked by an Administrator or Lighthouse. If this feature is not enabled, a user will be presented with a CAPTCHA challenge-response test after 5 consecutive failed login attempts.
Two Factor PIN Authentication Required	OFF	This feature provides Administrators with the ability to require a PIN during the login process for all users as well as the user's id and password credentials. The randomly generated PIN will be sent to the user's email address.
'Division' Field Name		This feature enables Administrators to change the name of the 'Division' field in CMS. The text in this field will appear on all pages and exports in place of the default field name 'Division'. This field is limited to 15 characters.

b. Manage Custom Fields – Allows an administrator to define up to three client defined fields for a report. These custom fields will appear on the Add/Edit/Show Incident Report pages and will be included in exports of incident report data. The following types of custom fields are available:

- Numeric - Integer
- Number - Decimal (2 decimal places)
- Numeric - Currency (2 decimal places)
- Date
- Text (maximum 255 characters)
- Dropdown List

c. Manage Inbox Messages - Allows an administrator to create messages that will be shown to users during sign on or during their session with the CMS. There are two types of messages: urgent and non-urgent. Messages can also be time sensitive with an optional From and To date range. User's messages are kept in their CMS Inbox until the user deletes them, the admin deletes the message from the Manage Message page or if the message is marked to be automatically deleted after a certain time period.

d. Manage Quick Response Messages – A total of five messages can be added as Quick Response Messages. This feature is accessed from the Settings tab by selecting Edit Record then clicking the Manage Quick Response Messages button on the right hand side of the page (see #4e).

e. Manage Reminder Notifications – Allows the company to create messages and set time intervals to keep Investigators active on a report. There are two types of reminder notifications: First Notification and a Subsequent Notification. The First reminder notification is only ever sent once after the first time interval has expired. The Subsequent Notification will continue to be sent after the expiration of each subsequent time interval as long as the report status has remained unchanged. This feature is accessed from the Settings tab by selecting Edit Record, then clicking the Manage Reminder Notification button on the right hand side of the page (see #5e).

f. Manage Security Settings – The Manage Security Settings allows an Administrator or user with Edit Settings access permission to set the following security features for their company:
    1. Password Policy - Allows an Administrator to customize the complexity of their CMS user passwords.
    2. IP Address Management - Allows an Administrator to manage which IP Addresses are allowed access to their CMS. By default, there are no restrictions on which IP addresses can access CMS.
    3. Email Link Management – Allows an Administrator to manage the amount of time before an emailed password link expires.
    4. Session Management - Allows an Administrator to determine how long a CMS user's session can be idle before they receive a warning and before their session is automatically terminated.
    5. Web API Access - Allows an Administrator to enable/disable access to their CMS programmatically (computer-to-computer). The Administrator can also set the access password to ensure secure access to their data. The current functionality via Web API access includes the ability to create a report and retrieve report information.

g. Manage Status Types - Allows an administrator to create custom report status types to meet their unique requirements. Lighthouse defines certain status types that are considered system statuses and which cannot be altered. The system statuses are Open, Pending, Closed, Unfounded, Archived, and Deleted.

For further information see the **CMS Company Setup Configurations** in our CMS help file.

Please email us at reports@lighthouse-services.com if you have questions.